Docket No. 250627US2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Jun EBATA

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: INFORMATION PROVIDING DEVICE, METHOD, PROGRAM AND RECORDING MEDIUM, AND USER AUTHENTICATION DEVICE, METHOD, PROGRAM AND RECORDING MEDIUM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2003-078993	March 20, 2003
Japan	2004-032085	February 9, 2004

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月２０日

出願番号
Application Number: 特願２００３－０７８９９３

[ST. 10/C]: [ＪＰ２００３－０７８９９３]

出願人
Applicant(s): 株式会社リコー

２００３年１１月２５日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０９７１５８

【書類名】　特許願
【整理番号】　0301261
【提出日】　平成15年 3月20日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F 15/00
【発明の名称】　ユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体
【請求項の数】　21
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　江畑　潤
【特許出願人】
　【識別番号】　000006747
　【氏名又は名称】　株式会社リコー
【代理人】
　【識別番号】　100070150
　【弁理士】
　【氏名又は名称】　伊東　忠彦
【手数料の表示】
　【予納台帳番号】　002989
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体

【特許請求の範囲】

【請求項１】　ユーザの認証を行う複数の認証手段を連携させる連携手段を有するユーザ認証装置であって、

前記連携手段は、

クライアントからのユーザの第一の認証要求に応じて、第一の認証手段に前記認証要求において指定された第一のユーザ識別情報に基づいて前記ユーザを認証させる第一の呼び出し手段と、

前記クライアントからの、前記第一の認証手段に認証されているユーザの第二の認証要求に応じて、前記第一のユーザ識別情報に予め対応づけられた、第二の認証手段における前記ユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手段と、

前記第二の認証手段に前記ユーザ識別情報検索手段が検索した前記第二のユーザ識別情報に基づいて前記ユーザを認証させる第二の呼び出し手段とを有することを特徴とするユーザ認証装置。

【請求項２】　前記第一のユーザ識別情報と前記第二のユーザ識別情報とを対応づけて管理するユーザ識別情報対応管理手段を更に有し、

前記ユーザ識別情報検索手段は、前記第一のユーザ識別情報に基づいて前記ユーザ識別情報対応管理手段から前記第二のユーザ識別情報を検索することを特徴とする請求項１記載のユーザ認証装置。

【請求項３】　前記連携手段は、前記第一のユーザ識別情報と前記第二のユーザ識別情報とを対応づけて管理するユーザ識別情報対応管理手段を更に有し、

前記ユーザ識別情報検索手段は、前記第一のユーザ識別情報に基づいて前記ユーザ識別情報対応管理手段から前記第二のユーザ識別情報を検索することを特徴とする請求項１記載のユーザ認証装置。

【請求項４】　前記複数の認証手段の中から前記第一の認証手段を識別する情報を管理する第一の認証手段識別情報管理手段と、

前記複数の認証手段の中から前記第二の認証手段を識別する情報を管理する第二の認証手段識別情報管理手段とを更に有し、

前記第一の呼び出し手段は、前記第一の認証手段識別情報管理手段に基づいて前記第一の認証手段として呼び出す認証手段を識別し、

前記第二の呼び出し手段は、前記第二の認証手段識別情報管理手段に基づいて前記第二の認証手段として呼び出す認証手段を識別することを特徴とする請求項１乃至３いずれか一項記載のユーザ認証装置。

【請求項５】　前記認証手段の呼び出し情報が登録された呼び出し情報管理手段を更に有し、

前記第一の呼び出し手段は、前記呼び出し情報管理手段に基づいて前記第一の認証手段を呼び出すことにより、前記第一の認証手段に前記ユーザを認証させ、

前記第二の呼び出し手段は、前記呼び出し情報管理手段に基づいて前記第二の認証手段を呼び出すことにより、前記第二の認証手段に前記ユーザを認証させることを特徴とする１乃至４いずれか一項記載のユーザ認証装置。

【請求項６】　前記第一の認証手段は、前記第一の認証手段が前記ユーザを認証したことを証明する電子的な証明書である第一のチケットを生成し、

前記第二の認証手段は、前記第二の認証手段が前記ユーザを認証したことを証明する電子的な証明書である第二のチケットを生成し、

前記ユーザ認証装置は、前記第一の認証要求に対する応答として、前記第一のチケットを前記クライアントに出力し、前記第二の認証要求に対する応答として、前記第二のチケットを前記クライアントに出力することを特徴とする請求項１乃至５いずれか一項記載のユーザ認証装置。

【請求項７】　前記連携手段は、前記第一のチケットと前記第二のチケットとをマージするマージチケットを生成するマージチケット生成手段を更に有し、

前記ユーザ認証装置は、前記第一の認証要求に対する応答として、前記第一のチケットがマージされた前記マージチケットを前記クライアントに出力し、前記第二の認証要求に対する応答として、前記第二のチケットがマージされた前記マージチケットを前記クライアントに出力することを特徴とする請求項６記載のユーザ認証装置。

【請求項８】　前記クライアントに出力されたマージチケットは、暗号化されていることを特徴とする請求項７記載のユーザ認証装置。

【請求項９】　前記マージチケット、前記第一のチケット及び前記第二のチケットにうち少なくとも一つは、有効期限を有することを特徴とする請求項６乃至８いずれか一項記載のユーザ認証装置。

【請求項１０】　前記マージチケット、前記第一のチケット及び前記第二のチケットのうち少なくとも一つは、改竄チェック用のコードを有することを特徴とする請求項６乃至９いずれか一項記載のユーザ認証装置。

【請求項１１】　前記マージチケット、前記第一のチケット及び前記第二のチケットのうち少なくとも一つは、それぞれが利用可能な対象を示す有効範囲を有することを特徴とする請求項６乃至１０いずれか一項記載のユーザ認証装置。

【請求項１２】　前記第一の認証手段は、パスワードに基づいてユーザの認証を行い、

前記第二の認証手段は、ユーザの指紋に基づいてユーザの認証を行うことを行うことを特徴とする請求項１乃至１１いずれか一項記載のユーザ認証装置。

【請求項１３】　前記連携手段は、

クライアントからの前記マージチケットの解読要求に応じ、前記マージチケットに記録されている情報を前記クライアントが解釈可能な形式にした認証情報データを前記クライアントに出力するチケット解読手段を更に有することを特徴とする請求項７乃至１２いずれか一項記載のユーザ認証装置。

【請求項１４】　前記チケット解読手段は、前記マージチケットにマージされている前記第一のチケットについては前記第一の認証手段に解読させ、前記マージチケットにマージされている前記第二のチケットについては前記第二の認証手段に解読させることを特徴とする請求項１３記載のユーザ認証装置。

【請求項１５】　前記連携手段の機能は、ＳＯＡＰのＲＰＣによって呼び出すことが可能なことを特徴とする請求項１乃至１４いずれか一項記載のユーザ認証装置。

【請求項１６】　ユーザの認証を行う複数の認証手段を連携させるユーザ認証装置におけるユーザ認証方法であって

クライアントからのユーザの第一の認証要求に応じて、第一の認証手段に前記認証要求において指定された第一のユーザ識別情報に基づいて前記ユーザを認証させる第一の呼び出し手順と、

前記クライアントからの、前記第一の認証手段に認証されているユーザの第二の認証要求に応じて、前記第一のユーザ識別情報に予め対応づけられた、第二の認証手段における前記ユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手順と、

前記第二の認証手段に前記ユーザ識別情報検索手順において検索された前記第二のユーザ識別情報に基づいて前記ユーザを認証させる第二の呼び出し手順とを有することを特徴とするユーザ認証方法。

【請求項１７】　前記ユーザ識別情報検索手順は、前記第一のユーザ識別情報に基づいて、前記第一のユーザ識別情報と前記第二のユーザ識別情報とを対応づけて管理するユーザ識別情報対応管理手段から前記第二のユーザ識別情報を検索することを特徴とする請求項１６記載のユーザ認証方法。

【請求項１８】　前記第一の呼び出し手順は、前記複数の認証手段の中から前記第一の認証手段を識別する情報を管理する第一の認証手段識別情報管理手段に基づいて前記第一の認証手段として呼び出す認証手段を識別し、

前記第二の呼び出し手順は、前記複数の認証手段の中から前記第二の認証手段を識別する情報を管理する第二の認証手段識別情報管理手段に基づいて前記第二の認証手段として呼び出す認証手段を識別することを特徴とする請求項１６又は１７記載のユーザ認証方法。

【請求項１９】　前記第一の呼び出し手順は、前記認証手段の呼び出し情報が登録された呼び出し情報管理手段に基づいて前記第一の認証手段を呼び出すことにより、前記第一の認証手段に前記ユーザを認証させ、

前記第二の呼び出し手順は、前記呼び出し情報管理手段に基づいて前記第二の認証手段を呼び出すことにより、前記第二の認証手段に前記ユーザを認証させることを特徴とする１６乃至１８いずれか一項記載のユーザ認証方法。

【請求項２０】　クライアントからのユーザの第一の認証要求に応じて、第一のユーザ識別情報に基づいて第一の認証手段に前記認証要求において指定され

た前記ユーザを認証させる第一の呼び出し手順と、

前記クライアントからの、前記第一の認証手段に認証されているユーザの第二の認証要求に応じて、前記第一のユーザ識別情報に予め対応づけられた、第二の認証手段における前記ユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手順と、

前記第二の認証手段に前記ユーザ識別情報検索手順において検索された前記第二のユーザ識別情報に基づいて前記ユーザを認証させる第二の呼び出し手順とをコンピュータに実行させるためのユーザ認証プログラム。

【請求項２１】　クライアントからのユーザの第一の認証要求に応じて、第一のユーザ識別情報に基づいて第一の認証手段に前記認証要求において指定された前記ユーザを認証させる第一の呼び出し手順と、

前記クライアントからの、前記第一の認証手段に認証されているユーザの第二の認証要求に応じて、前記第一のユーザ識別情報に予め対応づけられた、第二の認証手段における前記ユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手順と、

前記第二の認証手段に前記ユーザ識別情報検索手順において検索された前記第二のユーザ識別情報に基づいて前記ユーザを認証させる第二の呼び出し手順とをコンピュータに実行させるためのユーザ認証プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体に関し、特に複数の認証手段を連携させるユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体に関する。

【０００２】

【従来の技術】

情報システムの不正利用を防ぐために、各種アプリケーションは、ユーザの認証機能を有しているのが一般である。認証機能を実現するシステムの具体例とし

てアプリケーションの起動時にユーザＩＤとパスワードの入力を要求するパスワードシステムが挙げられる。ユーザＩＤとパスワードとを正しく入力したユーザには、アプリケーションの利用が許可され、以降、ユーザは、アプリケーションが提供する様々な機能を利用することができる。

【０００３】

【発明が解決しようとする課題】

しかしながら、ユーザの正当性がアプリケーションの起動時において確認できただけで、そのアプリケーションが提供するすべてのサービスに対する利用権限を与えるのは危険である。例えば、ユーザがアプリケーションを起動したまま席をはずすことがよくある。従って、悪意を持った他のユーザが、正当なユーザに成りすましてアプリケーションを利用することも考えられる。

【０００４】

かかる不正利用を防ぐため、例えば企業内の情報システムおいて管理されている機密情報に対してアクセスする際に、ユーザの認証を再度要求することにより、かかる機密情報に対するセキュリティを高めることができる。

【０００５】

この場合、起動時における認証の際に利用した認証エンジン（ユーザ認証を行うためのプログラム）と同一の認証エンジンを利用するよりも、例えば、起動時にはパスワード認証、機密情報へのアクセスの際には指紋認証といったように、全く別の認証エンジンを利用して認証を行ったほうが、より高度なセキュリティを確保することができる。

【０００６】

但し、二つ以上の認証エンジンを利用する場合、それぞれがお互いに独立していたのでは意味がない。即ち、一方において認証されたユーザと他方において認証されたユーザとが同一人物であるという保証がないからである。

【０００７】

従って、アプリケーションには、複数の認証エンジンを関連づける処理の実装が必要となる。

【０００８】

本発明は、上記の点に鑑みてなされたものであって、ユーザの同一性を保証しつつ複数の認証機能によってユーザを認証することができるユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体の提供を目的とする。

【０００９】

【課題を解決するための手段】

そこで上記課題を解決するため、本発明は、ユーザの認証を行う複数の認証手段を連携させる連携手段を有するユーザ認証装置であって、前記連携手段は、クライアントからのユーザの第一の認証要求に応じて、第一の認証手段に前記認証要求において指定された第一のユーザ識別情報に基づいて前記ユーザを認証させる第一の呼び出し手段と、前記クライアントからの、前記第一の認証手段に認証されているユーザの第二の認証要求に応じて、前記第一のユーザ識別情報に予め対応づけられた、第二の認証手段における前記ユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手段と、前記第二の認証手段に前記ユーザ識別情報検索手段が検索した前記第二のユーザ識別情報に基づいて前記ユーザを認証させる第二の呼び出し手段とを有することを特徴とする。

【００１０】

このようなユーザ認証装置では、第一の認証手段における第一のユーザ識別情報（ユーザＩＤ等）に予め対応づけられた第二のユーザ識別情報に基づいて、第二の認証手段にユーザの認証をさせるため、ユーザの同一性を保証しつつ複数の認証機能によってユーザを認証することができる。

【００１１】

また上記課題を解決するため、本発明は、上記ユーザ認証装置におけるユーザ認証方法、又はその方法をコンピュータに行なわせるためのプログラム及び前記プログラムを記録した記録媒体としてもよい。

【００１２】

【発明の実施の形態】

以下、図面に基づいて本発明の実施の形態を説明する。図１は、本発明の実施の形態における認証システムの構成例を示す図である。図１に示されるように、本実施の形態における認証システム１は、お互いにインターネットやＬＡＮ等の

ネットワークを介して接続されている認証サーバ１０と端末１０とを有している。

【００１３】

端末２０はユーザが利用するＰＣ（Personal Computer）等の端末であり、ＳＯＡＰプロキシ２２、クライアントアプリケーション２３、及び指紋読み取り装置ドライバ２４等と有している。ＳＯＡＰプロキシ２２は、認証サーバ１０との間でＳＯＡＰ（Simple Object Access Protocol）による通信を実現するためのモジュールであり、クライアントアプリケーション２３に対して、認証サーバ１０の機能を関数インタフェースとして透過的に提供するためのものである。

【００１４】

指紋読み取り装置ドライバ２４は、端末２０に接続された指紋読み取り装置２５に対するインタフェースをクライアントアプリケーション２３に提供するためのいわゆるドライバである。指紋読み取り装置２５は、ユーザの指紋を読み取るための装置である。

【００１５】

クライアントアプリケーション２３は、ユーザが直接操作するアプリケーションである。クライアントアプリケーション２３は、その起動時やその他のタイミングでユーザの認証が必要になった際に、ユーザに対して認証情報の入力を要求する。ユーザによって認証情報が入力されると、クライアントアプリケーション２３は、ＳＯＡＰプロキシ２２を介して認証サーバ１０にユーザの認証を要求する。

【００１６】

クライアントアプリケーション２３の種類については、特に限定されないが、少なくとも利用する際に認証を必要とするものである。本実施の形態においては、一般的なものと同様にメール機能等を有するグループウェアのクライアントアプリケーションを想定する。

【００１７】

なお、端末２０の位置づけ（認証サーバ１０のクライアント）としてＷｅｂサーバを想定してもよい。この場合、当該Ｗｅｂサーバは、Ｗｅｂアプリケーショ

ンとして実装されているクライアントアプリケーション２３と、ＳＯＡＰプロキシ２２を有し、ＳＯＡＰプロキシ２２によって認証サーバ１０との通信を行う。当該ＷｅｂサーバのＷｅｂクライアントとしてユーザが利用する端末には、Ｗｅｂブラウザと、指紋読み取り装置ドライバ２４が実装され、更に、指紋読み取り装置２５が接続されていればよい。こうすることによって、ユーザは、クライアントアプリケーション２３の機能を、端末のＷｅｂブラウザに表示されたＷｅｂページを通して利用することができる。

【００１８】

ユーザがクライアントアプリケーション２３を起動すると、クライアントアプリケーション２３は、まずユーザＩＤ（ユーザ識別情報）とパスワードの入力を要求する。ユーザがユーザＩＤとパスワードとを入力すると、クライアントアプリケーション２３は、ＳＯＡＰプロキシ２２を介して認証サーバ１０に対しユーザの認証を要求する。また、ユーザがクライアントアプリケーション２３上において、指紋認証が必要とされるセキュリティレベルの高い操作を行うとすると、クライアントアプリケーション２３は、ユーザに対して指紋の入力を要求する。ユーザが指紋読み取りデバイス２５によって指紋を入力すると、クライアントアプリケーション２３は、認証サーバ１０に対し、ユーザの認証を要求する。

【００１９】

一方、認証サーバ１０は、ユーザ認証のサービスをＷｅｂサービスとして提供するコンピュータであり、認証サービスモジュール１１がインストールされている。

【００２０】

認証サービスモジュール１１は、認証サーバ１０をユーザ認証サービスの提供をするための装置として機能させるためのソフトウェアであり、本実施の形態においては、ＳＯＡＰスタブ１２、プロバイダ呼び分け手段１３、認証プロバイダＡ１４、認証プロバイダＢ１５、パスワード・指紋マージプロバイダ１６、パスワード認証プロバイダ１７、指紋認証プロバイダ１８、及びマージ情報管理ＤＢ１９等から構成されている。

【００２１】

ＳＯＡＰスタブ１２は、端末２０との間でＳＯＡＰによる通信を実現するためのモジュールである。プロバイダ呼び分け手段１３は、端末２０に対して、後述する各種認証プロバイダに対する共通のインタフェースを提供するためのモジュールである。プロバイダ分け手段１３は、端末２０からユーザの認証要求を受けると、当該認証要求において指定された認証プロバイダを呼び出す。

【００２２】

認証プロバイダＡ１４、認証プロバイダＢ１５、パスワード・指紋マージプロバイダ１６、パスワード認証プロバイダ１７、及び指紋認証プロバイダ１８等は、「認証プロバイダ」と呼ばれるモジュールである。ここで、認証プロバイダとは、様々な認証エンジンを認証サービスモジュール１１に組み込むためのアダプタ、又は仲介者のような役割を果たすものである。なお、認証エンジンとは、ここでは実際にパスワードの照合や、指紋の照合等の認証処理を行うシステムをいう。

【００２３】

即ち、個々の認証エンジンは、それぞれ独自のインタフェース（プロトコル）を有している。一方、それぞれの認証エンジンにおける認証機能をＷｅｂサービスとして端末２０等に提供するにはプロバイダ呼び分け手段１３との間で規定される所定のインタフェースに従う必要がある。かかる個々の認証エンジンによる独自のプロトコルを吸収し、プロバイダ呼び分け手段１３に対して共通のインタフェースを提供するのが、認証プロバイダである。従って、新たな認証エンジンを認証サービスモジュール１１に組み込むには、認証プロバイダを一つ実装することになる。但し、認証プロバイダ自身が、認証エンジンとしての機能を有していてもよい。

【００２４】

具体的には、パスワード認証プロバイダ１７は、パスワード認証を行うための認証エンジンが実装されているサーバである外部認証サーバ４０の認証機能をＷｅｂサービスとして提供するための認証プロバイダである。また、指紋認証プロバイダ１８は、指紋認証ライブラリ１８１と指紋ＤＢ１８２とによる指紋認証機能をＷｅｂサービスとして提供するための認証プロバイダである。指紋認証ライ

ブラリ１８１は、指紋認証に関する機能を提供する関数群である。また、指紋ＤＢ１８２は、ユーザ毎の指紋特徴データが登録されているデータベースである。

【００２５】

認証プロバイダＡ１４及び認証プロバイダ１５は、様々な認証プロバイダを実装することが可能であることを示すための例示である。

【００２６】

パスワード・指紋マージプロバイダ１６は、認証プロバイダの一つであるが、認証エンジンに対する直接の仲介役として機能するものではないという点において、他の認証プロバイダとは異なる。即ち、パスワード・指紋マージプロバイダ１６は、パスワード認証プロバイダ１７と指紋認証プロバイダ１８とを連携させるための機能を提供する認証プロバイダである。なお、パスワード・指紋マージプロバイダ１６のように複数の認証プロバイダを連携させるための認証プロバイダを、以下「マージプロバイダ」と呼ぶ。

【００２７】

マージプロバイダによって連携される認証プロバイダは、それぞれ対等な関係ではなく主従関係を持つ。ここで、「主」となる認証プロバイダを「プライマリ（ｐｒｉｍａｒｙ）プロバイダ」と呼び、「従」となる認証プロバイダを「追加（ａｄｄｉｔｉｏｎａｌ）プロバイダ」と呼ぶこととする。連携された認証プロバイダの中で、プライマリプロバイダは一つであり、それ以外は全て追加プロバイダとなる。

【００２８】

ここで、主従の関係と表現したのは、追加プロバイダによって認証する際には、プライマリプロバイダによって既に認証されていることが前提となるからである。逆に、プライマリプロバイダによって認証する際は、追加プロバイダによって認証されていることは前提とならない。即ち、最初の認証に利用されるのがプライマリプロバイダであり、プライマリプロバイダによって認証が済んでいる場合において、更に特別な認証が必要な際に利用されるのが追加プロバイダというわけである。即ち、「連携」とは、複数の認証プロバイダを、上記の主従関係を持たせて結合することをいう。

【００２９】

本実施の形態においては、パスワード認証プロバイダ１７をプライマリプロバイダとし、指紋認証プロバイダ１８を追加プロバイダとした例について説明する。なお、マージプロバイダも、他の認証プロバイダと同様に、複数存在させてもよく、マージプロバイダによってマージする認証プロバイダの組み合わせは自由である。例えば、認証プロバイダＡ１４と認証プロバイダ１５とをマージする新たなマージプロバイダを定義してもよいし、パスワード・指紋マージプロバイダ１６に認証プロバイダＡ１４を更にマージさせてもよい。

【００３０】

マージ情報管理ＤＢ１９は、認証サーバ１０に実装されている認証プロバイダの一覧や、認証プロバイダ同士のマージの関係が登録されているデータベースである。

【００３１】

ここで、マージ情報管理ＤＢ１９を構成する各種テーブルについて説明する。図２は、マージ情報管理ＤＢを構成する認証プロバイダ管理テーブルの構成例を示す図である。図２の認証プロバイダ管理テーブル１９１（呼び出し情報管理手段）は、認証サーバ１０に登録されている認証プロバイダの一覧を管理しているテーブルであり、認証プロバイダ毎に、プロバイダ名、実装名、及び実装依存の初期化情報等が登録されている。

【００３２】

プロバイダ名は、認証プロバイダを一意に識別するための名前である。実装名は、例えば認証プロバイダの実装されているファイル名（ＥＸＥ名、ＤＬＬ名）、及び関数名等、認証プロバイダを呼び出すたに、あるいは起動するために必要となる情報である。実装依存の初期化情報は、認証プロバイダの呼び出し時、又は起動時に必要となる情報である。

【００３３】

このように、認証プロバイダ管理テーブル１９１によって、各認証プロバイダの呼び出し情報を管理することにより、プロバイダ呼び分け手段１３と認証プロバイダ、及びマージプロバイダと当該マージプロバイダにマージされる認証プロ

バイダとの間の結合を動的なものとすることができる。即ち、プロバイダ呼び分手段１３やマージプロバイダのソースコードには、呼び出し情報に依存する定義（例えば、ロードするＤＬＬ名や、呼び出す関数名等）をハードコーディングしておく必要はない。従って、新たな認証プロバイダを追加した場合でも、当該認証プロバイダが所定のインタフェースに従っている限り、プロバイダ呼び分け手段１３やマージプロバイダのソースコードを修正する必要はない。

【００３４】

本実施の形態においては、上述したように、認証プロバイダＡ１４、認証プロバイダＢ１５、パスワード・指紋マージプロバイダ１６、パスワード認証プロバイダ１７、及び指紋認証プロバイダ１８等が存在するため、それぞれのレコードが認証プロバイダ管理テーブル１９１に登録されている。
認証プロバイダ管理テーブル１９１によって、例えばプロバイダ呼び分け手段１３は、端末２０からユーザの認証要求があった際に、対応する認証プロバイダを呼び出すための手続きを知ることができる。

【００３５】

また、図３は、マージ情報管理ＤＢを構成するマージプロバイダ管理テーブルの構成例を示す図である。図３のマージプロバイダ管理テーブル１９２（第一の認証手段識別情報管理手段）は、認証プロバイダ管理テーブル１９１に登録されている認証プロバイダのうち、マージプロバイダである認証プロバイダを管理するテーブルであり、マージプロバイダ毎に、マージプロバイダ名及びプライマリプロバイダ名等が登録されている。

【００３６】

マージプロバイダ名は、マージプロバイダのプロバイダ名である。プライマリプロバイダ名は、当該マージプロバイダにおいてプライマリプロバイダとなっているプロバイダ名である。

【００３７】

マージプロバイダ管理テーブル１９２によって、マージプロバイダを識別することができる。また、マージプロバイダは、マージプロバイダ管理テーブル１９２によって、自身におけるプライマリプロバイダを識別する。従って、新たにマ

ージプロバイダを定義する場合や、既存のマージプロバイダのプライマリプロバイダを他の認証プロバイダに変更する場合は、マージプロバイダ管理テーブル１９２を変更すればよく、マージプロバイダのソースコードを修正する必要はない。

【００３８】

本実施の形態においては、パスワード・指紋マージプロバイダ１６がマージプロバイダであるため、パスワード・指紋マージプロバイダ１６に対応するレコードが登録されている。また、パスワード・指紋マージプロバイダ１６のプライマリプロバイダは、上述したようにパスワード認証プロバイダ１７であるため、パスワード・指紋マージプロバイダ１６のプライマリプロバイダのプロバイダ名として、パスワード認証プロバイダ１７のプロバイダ名が登録されている。

【００３９】

また、図４は、マージ情報管理ＤＢを構成する追加プロバイダ管理テーブルの構成例を示す図である。図３の追加プロバイダ管理テーブル１９３（第二の認証手段識別情報管理手段）は、各マージプロバイダに属する追加プロバイダを識別するためのテーブルであり、マージプロバイダ名及び追加プロバイダ名等のデータ項目を有する。マージプロバイダ名は、マージプロバイダのプロバイダ名である。追加プロバイダ名は、当該マージプロバイダにおいて追加プロバイダとなっているプロバイダ名である。

【００４０】

本実施の形態においては、パスワード・指紋マージプロバイダ１６の追加プロバイダは、指紋認証プロバイダ１８であるため、その旨が追加プロバイダ管理テーブル１９３に登録されている。なお、パスワード・指紋マージプロバイダ１６に更に追加プロバイダを追加する場合は、パスワード・指紋マージプロバイダ１６のプロバイダ名をマージプロバイダ名とし、更に追加プロバイダとして登録する認証プロバイダのプロバイダ名を追加プロバイダ名とした新たなレコードを、追加プロバイダ管理テーブル１９３に登録すればよい。

【００４１】

また、図５は、マージ情報管理ＤＢを構成する認証プロバイダマージテーブル

の構成例を示す図である。図５の認証プロバイダマージテーブル１９４（ユーザＩＤ対応管理手段）は、プライマリプロバイダにおけるユーザの識別情報（ユーザＩＤ等）と、追加プロバイダにおけるユーザＩＤとを対応づけるテーブルであり、マージプロバイダ名、プライマリＩＤ、追加プロバイダ名、及び追加ＩＤ等のデータ項目を有する。

【００４２】

マージプロバイダ名は、マージプロバイダのプロバイダ名である。プライマリＩＤとは、プライマリプロバイダに対応する認証エンジンにおいて、各ユーザに一意に割り当てられたユーザＩＤである。追加プロバイダ名は、追加プロバイダのプロバイダ名である。追加プロバイダ名の項目は、上述したように一つのマージプロバイダに複数の追加プロバイダを登録することが可能なため、後述する追加ＩＤがどの追加プロバイダにおけるものかを識別するために設けてあるものである。追加ＩＤは、追加プロバイダ名によって識別される追加プロバイダに対応する認証エンジンにおいて、各ユーザに一意に割り当てられたユーザＩＤである。

【００４３】

即ち、各ユーザを識別するためのコード体系は、各認証エンジンで異なるのが一般である。従って、それぞれの認証エンジンを有機的に連携させるためには、一方の認証エンジンにおけるユーザＩＤによって特定されるユーザの他方の認証エンジンにおけるユーザＩＤを特定するための手段が必要とされる。かかる手段を提供するのが認証プロバイダマージテーブル１９４である。なお、認証プロバイダマージテーブル１９４は、認証サービスモジュール１１に対して一つ実装してもよいし、マージプロバイダー一つに対して一つ、即ちマージプロバイダが有するように実装してもよい。

【００４４】

認証プロバイダ管理テーブル１９４について更に具体的に説明する。本実施の形態においては、パスワード・指紋マージプロバイダ１６のプライマリプロバイダであるパスワード認証プロバイダ１７は、上述したように外部認証サーバ４０に対応する認証プロバイダである。ここで、外部認証サーバ４０は、パスワード

認証を行う認証エンジンを実装したサーバであるため、例えば、図６に示されるユーザ管理テーブルを有している。

【００４５】

図６は、外部認証サーバにおけるユーザ管理テーブルの構成例を示す図である。図６のユーザ管理テーブル４１は、ユーザ毎に、ユーザＩＤ、パスワード、及び氏名等のユーザ情報を管理している。ここでユーザＩＤが、認証プロバイダマージテーブル１９４におけるプライマリＩＤに該当する。

【００４６】

一方、パスワード・指紋マージプロバイダ１６の追加プロバイダである指紋認証プロバイダ１８は、上述したように、指紋認証ライブラリ１８１と指紋ＤＢ１８２による指紋認証エンジンに対応する認証プロバイダである。ここで、指紋ＤＢ１８２は、例えば、図７に示される指紋特徴データ管理テーブルを有している。

【００４７】

図７は、指紋ＤＢを構成する指紋特徴データ管理テーブルの構成例を示す図である。図７の指紋特徴データ管理テーブル１８２１は、ユーザＩＤと指紋特徴データとをデータ項目として有する。ユーザＩＤは、指紋特徴データを一意に識別するための識別情報である。指紋特徴データは、指紋特徴データの実体である。ここで、ユーザＩＤが、マージテーブル１９４における追加ＩＤに該当する。

【００４８】

従って、認証プロバイダマージテーブル１９４より、外部認証サーバ４０においてユーザＩＤが０００１のユーザの指紋特徴データを特定することが可能となる。また、ユーザＩＤの対応づけを認証プロバイダマージテーブル１９４によって管理することにより、ユーザＩＤの対応づけに変更がある場合においても容易に対応することができる。

【００４９】

上述した、認証プロバイダ管理テーブル１９１、マージプロバイダ管理テーブル１９２、追加プロバイダ管理テーブル１９３、及び認証プロバイダマージテーブル１９４によって、マージプロバイダの動作に必要な情報が管理されることに

より、マージプロバイダのソースコードを汎用的なものとすることができる。即ち、唯一のソースコードから複数の異なるマージプロバイダを実現させることができる。

【００５０】

図８は、本発明の実施の形態における認証サーバのハードウェア構成例を示す図である。図８の認証サーバ１０は、それぞれバスBで相互に接続されているドライブ装置１００と、補助記憶装置１０２と、メモリ装置１０３と、演算処理装置１０４と、インタフェース装置１０５とを有するように構成される。

【００５１】

認証サーバ１０において認証サービスモジュール１１を実現するユーザ認証プログラムは、CD―ROM等の記憶媒体１０１によって提供される。ユーザ認証プログラムを記録した記憶媒体１０１は、ドライブ装置１００にセットされると、ユーザ認証プログラムが記憶媒体１０１からドライブ装置１００を介して補助記憶装置１０２にインストールされる。

【００５２】

補助記憶装置１０２は、インストールされたユーザ認証プログラムを格納すると共に、必要なファイルやデータ等を格納する。例えば補助記憶装置１０２は、ユーザ認証プログラムの処理に必要な、上述した各種テーブルを格納している。

【００５３】

メモリ装置１０３は、認証サーバ１０の起動時等、ユーザ認証プログラムの起動指示があった場合に、補助記憶装置１０２からユーザ認証プログラムを読み出して格納する。演算処理装置１０４は、メモリ装置１０３に格納されたユーザ認証プログラムに従って認証サーバ１０に係る機能を実行する。インタフェース装置１０５は例えばモデム、ルータ等で構成され、ＬＡＮ又はインターネット等のネットワークに接続するために用いられる。

【００５４】

以下、図１の認証サーバ１０の処理手順について説明する。なお、以下の説明において、プライマリプロバイダを利用した認証を「プライマリ認証」と、追加プロバイダを利用した認証を「追加認証」という。図９は、プライマリ認証の際

の認証サーバの処理を説明するためのシーケンス図である。

【００５５】

ユーザがクライアントアプリケーション２３を利用すべくクライアントアプリケーション２３を起動すると、クライアントアプリケーション２３は、ユーザに対しユーザＩＤ及びパスワードの入力を要求する。ユーザがユーザＩＤ及びパスワードを入力すると、クライアントアプリケーション２３は、プロバイダ呼び分け手段１３が提供する認証関数（Authenticate(プロバイダ名、ドメイン名、ユーザＩＤ、パスワード)）をＳＯＡＰのＲＰＣで呼び出すことにより、認証サーバ１０に対しユーザの認証を要求する（Ｓ１１）。なお、認証関数の各引数の意味は以下の通りである。

【００５６】

プロバイダ名は、認証に利用する認証プロバイダであるであり、ここではパスワード・指紋マージプロバイダ１６のプロバイダが指定される。ドメイン名は端末２０が属するドメインのドメイン名である。ユーザＩＤ以降は、認証に利用する認証プロバイダによって、指定する値が異なる。本実施の形態では、パスワード・指紋マージプロバイダ１６のプライマリプロバイダは、パスワード認証プロバイダ１７であるため、パスワード認証に必要な情報としてユーザに入力させたユーザＩＤとパスワードが指定される。

【００５７】

ステップＳ１１に続いてステップＳ１２に進み、ＲＰＣによって認証関数が呼び出されたプロバイダ呼び分け手段１３は、認証関数の引数のプロバイダ名によって指定されている認証プロバイダを呼び出すために必要な情報を認証プロバイダ管理テーブル１９１から取得し、当該認証プロバイダを呼び出す。ここでは、パスワード・指紋マージプロバイダ１６が呼び出される。

【００５８】

ステップＳ１２に続いてステップＳ１３に進みパスワード・指紋マージプロバイダ１６は、自己のプライマリプロバイダとして登録されている認証プロバイダをマージプロバイダ管理テーブル１９２に基づいて識別し、当該プライマリプロバイダの認証関数（Authenticate（ドメイン名、ユーザＩＤ、パスワード））を

呼び出す。ここでは、パスワード認証プロバイダ１７の認証関数呼び出される。なお、プライマリプロバイダの認証関数の各引数の値は、ディパッチャ１３の認証関数が呼び出される際に指定された値が引き継がれる。

【００５９】

ステップＳ１３に続いてステップＳ１４に進み、パスワード認証プロバイダ１７は、外部認証サーバ４０を利用してパスワード認証を実行する。ユーザが正当であることが確認されたらステップＳ１５に進み、パスワード認証プロバイダはチケットを生成する。

【００６０】

ここで、チケットについて説明する。本実施の形態におけるチケットとは、認証にパスしたユーザ（クライアント）に対して認証プロバイダが発行する、当該ユーザが認証されたことを証明する電子的な証明書をいう。チケットを発行されたクライアントは、文書管理サーバ等、所定のサーバを利用する際にチケットを提示することにより当該サーバを利用する権限を得ることができる。

【００６１】

図１０は、通常のチケットのデータ構造の例を示す図である。図１０に示されるようにチケット５０１は、チケットＩＤ、有効範囲、認証プロバイダ名、有効期限、認証ドメイン名、認証ユーザＩＤ、主なユーザ属性のリスト、及びＭＩＣ等から構成される。

【００６２】

チケットＩＤは、発行されたチケットを一意に識別するためのコードである。有効範囲については後述する。認証プロバイダ名は、実際に認証を行った（チケットを発行した）認証プロバイダのプロバイダ名である。有効期限は、当該チケットが有効な期限である。認証ドメイン名及び認証ユーザＩＤは、認証を受けユーザに対応するドメイン名及びユーザＩＤである。主なユーザ属性リストは、認証を受けたユーザの様々な属性（例えば、所属、役職等）である。ＭＩＣは、当該チケットが途中で改竄されていないかを確認するためのコードである。

【００６３】

なお、チケットには、認証チケットとマスタチケットとがある。認証チケット

とは、限られた範囲でのみ利用可能なチケットである。限られた範囲とは、所定のドメイン内でのみ利用可能であることや、所定のシステム又はサーバのみで利用可能であることを意味する。例えば、文書管理システムのみで利用可能な認証チケットは、他のシステムでは利用できない。従って、万が一認証チケットを盗まれた場合は、ユーザが受ける被害盗まれた認証チケットが有効な範囲のみに限られる。

【００６４】

これに対し、マスタチケットとは、チケットに対応しているシステムの全範囲に渡って利用可能な万能のチケットである。認証チケットの発行を要求する際には、マスタチケットを提示する必要がある。但し、その万能性ゆえ、マスタチケットを盗まれた場合には、被害はチケットに対応しているシステムの全範囲に及ぶ可能性がある。従って、マスタチケットは、認証チケットの発行要求等、マスタチケットの提示が必須の場合のみ利用し、通常のサービスを受ける際には、認証チケットを利用するといった使い分けをすることにより、より高度なセキュリティを確保することができる。

【００６５】

上記の説明において保留にした、チケットの構成要素である有効範囲は、かかる分類を識別するためのものである。即ち、当該チケットがマスタチケットである場合は、有効範囲には「マスタ」と記録され、認証チケットである場合は、当該認証チケットが有効な範囲を識別するための名称（ドメイン名、サーバ名等）が記録される。

【００６６】

なお、図９において、ステップＳ１１からステップＳ１９まではマスタチケットを発行するための処理に係り、ステップＳ２０からステップＳ２９まではマスタチケットを提示して認証チケットを得るための処理に係る。

【００６７】

また、別の観点から、チケットにはｉｎｎｅｒチケットとｏｕｔｅｒチケットとがある。ｉｎｎｅｒチケットとは、その名の通り内部のチケット、即ち、認証サーバ１０の内部におけるチケットに対する呼び名である。これに対しｏｕｔｅ

ｒチケットとは、認証管理サーバ１０の外部におけるチケットに対する呼び名である。即ち、ｉｎｎｅｒチケットとｏｕｔｅｒチケットとの違いは、記録されている情報の内容が異なるといった本質的なものではない。認証サーバ１０から端末２０等へチケットが送信される際等に、チケットは、ｉｎｎｅｒチケットからｏｕｔｅｒチケットに変換される。一方、認証サーバ１０が端末２０等からｏｕｔｅｒチケットを受信した際には、チケットは、ｏｕｔｅｒチケットからｉｎｎｅｒチケットへと変換される。ここで変換の具体例としては、暗号化が挙げられる。即ち、ｉｎｎｅｒチケットを暗号化したものがｏｕｔｅｒチケットという関係である。チケットを暗号化することにより、例えチケットが盗まれた場合でも、その内容が不正に利用されることを防止することができる。

【００６８】

更に、本実施の形態においては、チケットをその発行元によって、プライマリチケットと追加チケットとに呼び分ける。プライマリチケットとは、プライマリプロバイダが発行したチケットをいい、追加チケットとは、追加プロバイダが発行したチケットをいう。

【００６９】

ステップＳ１５においてパスワード認証プロバイダ１７は、ｉｎｎｅｒ型のマスタチケットを生成する。また、パスワード認証プロバイダ１７は、プライマリプロバイダであるため、生成したチケットはプライマリチケットに分類される。よって、以下、ステップＳ１５においてパスワード認証プロバイダ１７が生成したチケットを「マスタプライマリチケット」という。

【００７０】

マスタプライマリチケットの各項目には以下のような値が記録されている。

【００７１】

有効範囲：「マスタ」

認証プロバイダ名：「パスワード認証プロバイダ」

有効期限：２００２/ＭＭ/ＤＤ

認証ドメイン名：＜認証関数の引数に指定されたドメイン名＞

認証ユーザＩＤ：＜認証関数の引数に指定されたユーザＩＤ＞

ステップＳ１５に続いてステップＳ１６に進み、パスワード認証プロバイダ１７は、認証関数の戻り値として、生成したマスタプライマリチケットをパスワード・指紋マージプロバイダ１６に出力する。ステップＳ１６に続いてステップＳ１７に進み、パスワード・指紋マージプロバイダ１６は、マージ（Ｍｅｒｇｅ）チケットを生成し、マージチケットにマスタプライマリチケットをマージする。

【００７２】

図１１は、マージチケットのデータ構造の例を示す図である。図１１に示されるマージチケット５０２は、複数のチケットをマージするためのチケットであり、チケット種別、認証プロバイダ名、有効期限、プライマリプロバイダ名、プライマリチケット、追加チケットのリスト、及びＭＩＣ等から構成される。

【００７３】

チケット種別は、図１０に示される通常のチケット５０１における「有効範囲」と同義である。認証プロバイダ名は、当該マージチケットを発行した認証プロバイダ名である。従って、ここでは認証プロバイダ名にはパスワード・指紋マージプロバイダ１６のプロバイダ名が記録される。有効期限は、当該マージチケットの有効期限である。プライマリプロバイダ名は、当該マージチケットにマージされたプライマリチケットを発行したプライマリプロバイダのプロバイダ名である。従って、ここではパスワード認証プロバイダ１６のプロバイダ名が記録される。プライマリチケットは、プライマリプロバイダが発行した、プライマリチケットそのものが記録される。従って、ここではパスワード認証プロバイダ１６が発行したマスタプライマリチケットが記録される。追加チケットのリストは、追加プロバイダの発行する追加チケットが記録される。但し、この時点では、まだ追加プロバイダによる認証は実行されていないため、追加チケットのリストは空である。ＭＩＣは、通常のチケット５０１におけるＭＩＣと同義である。

【００７４】

なお、マージチケットについても、マスタチケット／認証チケットの区別と、ｉｎｎｅｒチケット／ｏｕｔｅｒチケットの区別とがあるが、ステップＳ１７で生成されるのは、ｉｎｎｅｒ型でかつマスタ型のマージチケットである。従って、ステップＳ１７においえパスワード・指紋マージプロバイダ１６が生成したチ

ケットを、以下「マスタマージチケット」という。

【００７５】

ステップＳ１７に続いてステップＳ１８に進み、パスワード・指紋マージプロバイダ１６は、生成したマスタマージチケットをプロバイダ呼び分け手段１３に対して出力する。ステップＳ１８に続いてステップＳ１９に進み、プロバイダ呼び分け手段１３は、ｉｎｎｅｒ型のマスタマージチケットをｏｕｔｅｒ型に変換（例えば暗号化）し、ｏｕｔｅｒ型に変換されたマスタマージチケットをクライアントアプリケーション２３に送信する。

【００７６】

ステップＳ１９が完了した時点で、クライアントアプリケーション２３は、マスタマージチケットを取得したことになる。上述したようにマスタチケットは、万能のチケットであるため、このままマスタマージチケットを利用して他のシステムを利用することも可能であるが、マスタチケットをネットワーク上に頻繁に流通させるのは、セキュリティ上好ましくない。従って、クライアントアプリケーション２３は、プロバイダ呼び分け手段１３の認証チケット生成関数（createAuthTicket（マスタマージチケット））をＳＯＡＰのＲＰＣで呼び出すことにより、利用対象とするシステムに対してのみ有効な認証チケットの生成を認証サーバ１０に要求する（Ｓ２０）。なお、認証チケット生成関数の引数には、ステップＳ１９で取得した、ｏｕｔｅｒ型のマスタマージチケットを指定する。

【００７７】

ステップＳ２０に続いてステップＳ２１に進み、認証チケット生成関数が呼び出されたプロバイダ呼び分け手段１３は、ｏｕｔｅｒ型のマスタマージチケットをｉｎｎｅｒ型に変換（暗号化を解除）する。更に、プロバイダ呼び分け手段１３は、マスタマージチケットの「認証プロバイダ名」を確認することにより、マスタマージチケットを発行した認証プロバイダを判別する。

【００７８】

ステップＳ２１に続いてステップＳ２２に進み、プロバイダ呼び分け手段１３は、マスタマージチケットの発行元である認証プロバイダを呼び出す。従って、ここではパスワード・指紋マージプロバイダ１６が呼び出される。ステップＳ２

２に続いてステップＳ２３に進み、パスワード・指紋マージプロバイダ１６は、マスタマージチケットの正当性を有効期限及びＭＩＣ等により確認する。

【００７９】

ステップＳ２３に続いてステップＳ２４に進み、パスワード・指紋マージプロバイダ１６は、マスタマージチケットにマージされているプライマリチケットを発行したプライマリプロバイダの認証チケット生成関数（createAuthTicket（マスタプライマリチケット））を呼び出す。従って、ここではパスワード認証プロバイダ１７の認証チケット生成関数が呼び出される。なお、パスワード認証プロバイダ１７の認証チケット生成関数の引数には、マスタマージチケットから取り出したマスタプライマリチケットが指定される。

【００８０】

ステップＳ２４に続いてステップＳ２５に進み、パスワード認証プロバイダ１７は、引数に指定されたマスタプライマリチケットの正当性を有効期限及びＭＩＣ等により確認し、認証チケットを生成する。認証チケットのデータ構造は、図１０において説明した通りであり、マスタプライマリチケットと同様に各項目に値が記録される。但し、「有効範囲」については、マスタプライマリチケットと異なり、当該認証チケットが有効なサーバ名又はドメイン名等が記録される。

【００８１】

なお、ここで生成された認証チケットについても、プライマリプロバイダであるパスワード認証プロバイダ１７が生成したものであるという意味で、プライマリチケットに分類される。従って、以下、ステップＳ２５においてパスワード認証プロバイダ１７が生成した認証チケットを「認証プライマリチケット」という。

【００８２】

ステップＳ２５に続いてステップＳ２６に進み、パスワード認証プロバイダ１７は、認証チケット生成関数の戻り値として、生成した認証プライマリチケットをパスワード・指紋マージプロバイダ１６に出力する。ステップＳ２６に続いてステップＳ２７に進み、パスワード・指紋マージプロバイダ１６は、マージチケットを生成し、マージチケットに認証プライマリチケットをマージする。

【００８３】

ここで、パスワード・指紋マージプロバイダ１６が生成するマージチケットは、有効範囲が限定された認証チケットである。よって、ステップＳ２７においてパスワード・指紋マージプロバイダ１６が生成したマージチケットを、以下「認証マージチケット」という。

【００８４】

ステップＳ２７に続いてステップＳ２８に進み、パスワード・指紋マージプロバイダ１６は、生成した認証マージチケットをプロバイダ呼び分け手段１３に対して出力する。ステップＳ２８に続いてステップＳ２９に進み、プロバイダ呼び分け手段１３は、ｉｎｎｅｒ型の認証マージチケットをｏｕｔｅｒ型に変換し、ｏｕｔｅｒ型に変換された認証マージチケットをクライアントアプリケーション２３に送信する。

【００８５】

以上により、クライアントアプリケーション２３は、マスタマージチケットに次いで認証マージチケットを取得したことになる。従って、クライアントアプリケーション２３は、認証マージチケットの有効なサーバに対して認証マージチケットを提示することにより、当該サーバのサービスを利用することができる。但し、上記においては、プライマリプロバイダ（パスワード認証プロバイダ１７）による認証しか受けていないため、クライアントアプリケーション２３に与えられた権限は、プライマリプロバイダによって認証を受けた範囲に限られる。

【００８６】

ここでいう「認証を受けた範囲」における「範囲」とは、チケット５０１のデータ項目である「有効範囲」における「範囲」と異なる概念である。「有効範囲」における範囲は、例えば、当該チケットは、サーバＡとサーバＢとで有効であるというように、利用可能な対象を示す意味での範囲である。一方、「認証を受けた範囲」における範囲は、当該チケットは、プライマリプロバイダのみに認証を受けており、追加プロバイダには認証されていないといったように、認証を受けたレベルを示すものである。たとえていえば、前者は平面的な広がりにおける範囲をいい、後者は深さ方向における範囲をいう。

【００８７】

以下、ユーザが、更に”深い”、即ち、本人であることを更に保障するための追加認証を受ける際の処理について説明する。図１２及び図１３は、追加認証の際の認証サーバの処理を説明するためのシーケンス図である。クライアントアプリケーション２３のユーザが、パスワード認証プロバイダ１７によって認証を受けただけでは、利用できないサービスを利用しようとした場合を想定する。例えば、重要な機密情報にアクセスしようとした場合、又は、部下の承認要求に対して承認を実行しようとした場合などがいい例である。ユーザがかかる処理要求を行った場合に、本実施の形態におけるクライアントアプリケーション２３は、ユーザに対し指紋の入力を要求する。

【００８８】

但し、ここではユーザＩＤの入力は必要とされない。一般に、認証を受ける際には、ユーザＩＤ等のユーザを一意に特定するための情報ユーザと、パスワード、指紋等のユーザが本人であることを保証するための情報を入力が必要である。ユーザＩＤの入力のみでは、ユーザが本人であるかを判断することができず、パスワードや指紋の入力のみでは、誰のパスワード又は指紋であるのか判断することができないからである。従って、通常であれば、ここにおいて、ユーザは指紋と共に、ユーザＩＤの入力が要求されるはずである。しかし、本実施の形態におけるパスワード・指紋マージプロバイダ１６は、詳細については後述されるが、既にプライマリ認証の際に入力されたユーザＩＤ（プライマリＩＤ）に基づいて、当該ユーザの追加認証におけるユーザＩＤ（追加ＩＤ）を特定するため、ユーザに、追加認証の際にユーザＩＤの入力を要求する必要がないのである。

【００８９】

ユーザが指紋読み取りデバイス２５に指紋を読み取らせると、クライアントアプリケーション２３は、プロバイダ呼び分け手段１３の追加認証関数（addAuthenticate（マスタマージチケット、追加認証プロバイダ名、指紋特徴データ）をＳＯＡＰのＲＰＣによって呼び出すことにより、認証サーバ１０に対して追加認証を要求する（Ｓ４１）。

【００９０】

なお、追加認証関数の引数の意味は、以下の通りである。マスタマージチケットには、マスタプライマリチケットがマージされている既に取得済みのマスタマージチケットを指定する。追加認証プロバイダ名には、追加認証を要求する追加プロバイダのプロバイダ名を指定する。従って、ここでは指紋認証プロバイダ１８のプロバイダ名を指定する。指紋特徴データには、指紋読み取りデバイス２５で読み取った指紋特徴データを指定する。

【００９１】

ステップＳ４１に続いてステップＳ４２に進み、追加認証関数が呼び出されたプロバイダ呼び分け手段１３は、マスタマージチケットの「認証プロバイダ名」を確認することにより、マスタマージチケットを発行した認証プロバイダを判別する。なお、本ステップ以降の説明においては、チケットについてのｏｕｔｅｒ形、ｉｎｎｎｅｒ型の区別については省略する。

【００９２】

ステップＳ４２に続いてステップＳ４３に進み、プロバイダ呼び分け手段１３は、マスタマージチケットの発行元である認証プロバイダを呼び出す。従って、ここではパスワード・指紋マージプロバイダ１６が呼び出される。ステップＳ４３に続いてステップＳ４４に進み、パスワード・指紋マージプロバイダ１６が、マスタマージチケットからマスタプライマリチケットを取り出し、マスタプライマリチケットの所有者であるユーザのユーザＩＤ（プライマリＩＤ）の取得をプライマリプロバイダであるパスワード認証プロバイダ１７に要求すると、パスワード認証プロバイダ１７は、マスタプライマリチケットの正当性を確認すると共に、マスタプライマリチケットから認証ユーザＩＤを取り出し、パスワード・指紋マージプロバイダ１６に対して取り出した認証ユーザＩＤをプライマリＩＤとして出力する。

【００９３】

ステップＳ４４に続いてステップＳ４５に進み、パスワード・指紋マージプロバイダ１６は、パスワード認証プロバイダ１７から取得したプライマリＩＤをキーとして、認証プロバイダマージテーブル１９４を検索し、プライマリＩＤに対応する追加ＩＤを取得する。なお、ここで取得された追加ＩＤは、指紋ＤＢ１８

２の指紋特徴データ管理テーブル１８２１におけるユーザＩＤに該当する。

【００９４】

ステップＳ４５に続いてステップＳ４６に進み、パスワード・指紋マージプロバイダ１６は、追加認証関数の引数で指定された追加認証プロバイダ名によって特定される追加プロバイダの認証関数（Authenticate（追加ＩＤ、指紋特徴データ））を呼び出す。従って、ここでは指紋認証プロバイダ１８の認証関数が呼び出される。

【００９５】

ステップＳ４６に続いてステップＳ４７に進み、認証関数が呼び出された指紋認証プロバイダ１８は、引数に指定された追加ＩＤ（ユーザＩＤ）をキーに指紋ＤＢ１８２から指紋特徴データを取り出し、取り出した指紋特徴データと、認証関数の引数に指定された指紋特徴データとを照合する。

【００９６】

ここで、認証関数の引数に指定された指紋特徴データは、追加認証を要求したユーザのものである。一方、ステップＳ４７において指紋ＤＢ１８２から取り出された指紋特徴データは、プライマリ認証を受けたユーザのユーザＩＤであるプライマリＩＤをキーとして認証プロバイダマージテーブル１９４から検索した追加ＩＤに対応するものである。

【００９７】

従って、二つの指紋特徴データが一致することにより、追加認証を要求したユーザが、指紋ＤＢ１８２登録されているユーザであることと共に、プライマリ認証を受けたユーザと追加認証を受けたユーザとが同一人物であることが保証される。

【００９８】

また、二つの認証をパスしたことで、クライアントアプリケーション２３のユーザが本人であることの保証がより高まったといえる。

【００９９】

従って、指紋認証プロバイダ１８は、自らが認証したことを証明するマスタチケットを生成する（Ｓ４８）。なお、指紋認証プロバイダ１８は、追加プロバイ

ダであるため、指紋認証プロバイダ１８が発行するチケットは追加チケットであるといえる。よって、ステップＳ４８において指紋認証プロバイダ１８が生成したマスタチケットを、以下「マスタ追加チケット」という。

【０１００】

なお、ここで生成されたマスタ追加チケットの「認証プロバイダ名」には、指紋認証プロバイダ１８の認証プロバイダ名が記録され、認証ユーザＩＤには、指紋ＤＢ１８２におけるユーザＩＤが記録される。

【０１０１】

ステップＳ４８に続いてステップＳ４９に進み、指紋認証プロバイダ１８は、生成したマスタ追加チケットをパスワード・指紋マージプロバイダ１６に出力する。ステップＳ４９に続いてステップＳ５０に進み、パスワード・指紋マージプロバイダ１６は、既にマスタプライマリチケットがマージされているマスタマージチケットにマスタ追加チケットをマージする。

【０１０２】

ステップＳ５０に続いてステップＳ５１に進み、パスワード・指紋マージプロバイダ１６は、マスタ追加チケットを更にマージしたマスタマージチケットをプロバイダ呼び分け手段１３に出力する。ステップＳ５１に続いてステップＳ５２に進み、プロバイダ呼び分け手段１３は、クライアントアプリケーション２３に対してマスタマージチケットを送信する。この時点でクライアントアプリケーション２３は、追加チケットがマージされた（追加認証を受けた）更に信頼性の高いマスタマージチケットを入手したことになる。

【０１０３】

ステップＳ５２に続いて図１３のステップＳ５３に進み、以降は図９のステップＳ２０以降の処理と同様に、クライアントアプリケーション２３が認証チケットを取得するための処理である。従って、ステップＳ５３からステップＳ５９までは、図９のステップＳ２０からステップＳ２６までの処理と同様である。即ち、クライアントアプリケーション２３によるプロバイダ呼び分け手段１３の認証チケット生成関数（createAuthTicket（マスタマージチケット））の呼び出しに基づいて（Ｓ５３）、パスワード認証プロバイダ１７によって認証プライマリチ

ケットが生成され、パスワード・指紋マージプロバイダ１６に出力される（Ｓ５４～Ｓ５９）。

【０１０４】

ここで、認証プライマリチケットを受け取ったパスワード・指紋マージプロバイダ１６は、マスタマージチケットが追加認証されたものであるのか、即ち、マスタマージチケットにマスタ追加チケットがマージされているか否かを判断する。

【０１０５】

マスタマージチケットにマスタ追加チケットがマージされていない場合は、図９の場合と同様に認証プライマリチケットがマージされた認証マージチケットがクライアントアプリケーション２３に送信される（Ｓ６０）。しかし、今回は、既にマスタマージチケットについて追加認証を受けている。従って、パスワード・指紋マージプロバイダ１６は、追加プロバイダからも認証チケットを取得するため、マスタマージチケットにマージされている追加チケットを発行した追加プロバイダの認証チケット生成関数（createAuthTicket（マスタ追加チケット））を呼び出す（Ｓ６１）。従って、ここでは指紋認証プロバイダ１８の認証チケット生成関数が呼び出される。なお、指紋認証プロバイダ１８の認証チケット生成関数の引数には、マージチケットから取り出したマスタ追加チケットが指定される。

【０１０６】

ステップＳ６１に続いてステップＳ６２に進み、指紋認証プロバイダ１８は、引数に指定されたマスタ追加チケットの正当性を有効期限及びＭＩＣ等により確認し、正当である場合は、認証チケット（以下、「認証追加チケット」という。）を生成する。

【０１０７】

ステップＳ６２に続いてステップＳ６３に進み、指紋認証プロバイダ１８は、認証チケット生成関数の戻り値として、生成した認証追加チケットをパスワード・指紋マージプロバイダ１６に出力する。ステップＳ６３に続いてステップＳ６４に進み、パスワード・指紋マージプロバイダ１６は、認証マージチケットを生

成し、ステップＳ５９で取得した認証プライマリチケットと、ステップＳ６３で取得した認証追加チケットとを認証マージチケットにマージする。

【０１０８】

ステップＳ６４に続いてステップＳ６５に進み、以降、認証マージチケットがクライアントアプリケーション２３に送信される（Ｓ６６）。

【０１０９】

以上により、クライアントアプリケーション２３は、図９のステップＳ２９において入手した認証マージチケットよりも信頼性が高い、追加認証された認証マージチケットを取得したことになる。従って、クライアントアプリケーション２３は、認証マージチケットの有効なサーバに対して認証マージチケットを提示することにより、更にセキュリティレベルの高いサービスを利用することができる。

【０１１０】

なお、図１２のステップＳ４１においてクライアントアプリケーション２３が呼び出すプロバイダ呼び分け手段１３の追加認証関数（addAuthenticate）は、引数として追加認証プロバイダ名の指定を要求している。これは、クライアント主導で次に追加認証を行わせる追加プロバイダが決定されることを示している。

【０１１１】

即ち、上述においては、パスワード・指紋マージプロバイダ１６の追加プロバイダとして指紋認証プロバイダ１８一つのみが定義されている例について説明したが、追加プロバイダ管理テーブル１９３と認証プロバイダマージテーブル１９４に新たな認証プロバイダの情報を追加すれば、パスワード・指紋マージプロバイダ１６に複数の追加プロバイダを定義することも可能である。

【０１１２】

かかる追加プロバイダが複数ある場合に、上述の例では、追加認証を行わせる追加プロバイダの順番は、追加認証関数を呼び出すクライアントの指定に従うことになる。

【０１１３】

しかし、追加認証を行わせる追加プロバイダの順番は、マージプロバイダ（パ

スワード・指紋マージプロバイダ１６）に判断させるようにしてもよい。例えば、追加プロバイダ管理テーブル１９３に新たなデータ項目として「順番」を追加し、「順番」項目に追加認証を行わせる順番を登録しておく。クライアントアプリケーション２３から追加認証の要求があった場合は、マージプロバイダが追加プロバイダ管理テーブル１９３の「順番」項目を確認することにより、次に呼び出す追加プロバイダを決定する。

【０１１４】

この場合は、追加認証関数の引数から追加プロバイダ名を削除してしまってもよいし、そのまま指定させるようにしてもよい。そのまま指定させるようにした場合は、追加認証関数の引数に指定された追加プロバイダ名と、マージプロバイダが判断した追加プロバイダ名とを比較することにより、サーバ側とクライアント側とのフェーズが一致しているか否かを確認することができる。

【０１１５】

次に、認証サーバ１０が発行したチケットがどのように利用されるかについて説明する。図１４は、チケットの第一の利用方法を説明するためのシーケンス図である。図１４において、クライアント３０は、クライアントアプリケーション２３でもよいが、ここでは、クライアントアプリケーション２３等に所定のサービスを提供するサーバであるとする。そして、クライアント３０がクライアントアプリケーション２３からサービスの利用要求と共に認証マージチケットの提示を受けた場合を想定する。なお、クライアント３０は、クライアントアプリケーション２３に対してはサーバであるが、認証サーバ３０に対しては「クライアント」であるため、図１４においてクライアント３０と表現している。

【０１１６】

認証マージチケットの提示を受けたクライアント３０は、自分自身ではチケットの中身を解釈することができない。クライアントアプリケーション２３から提示された認証マージチケットは暗号化（ｏｕｔｅｒ型）されており、また、クライアント３０は、チケットの構造については関知しないからである。

【０１１７】

よって、クライアント３０は、ステップＳ１０１において、プロバイダ呼び分

け手段１３の提供するチケット解読関数（decodeTicket（認証マージチケット））を呼び出すことにより、認証マージチケットの解読を認証サーバ１０に要求する。なお、チケット解読関数の引数には、クライアントアプリケーション２３から提示（送信）された認証マージチケットを指定する。

【０１１８】

ステップＳ１０１に続いてステップＳ１０２に進み、チケット解読関数が呼び出されたプロバイダ呼び分け手段１３は、認証マージチケットを発行した認証プロバイダを判別する。

【０１１９】

ステップＳ１０２に続いてステップＳ１０３に進み、プロバイダ呼び分け手段１３は、認証マージチケットの発行元であるパスワード・指紋マージプロバイダ１６を呼び出す。ステップＳ１０３に続いてステップＳ１０４に進み、パスワード・指紋マージプロバイダ１６は、認証マージチケットの正当性を有効期限及びＭＩＣ等により確認し、認証マージチケットにマージされているプライマリチケットを発行したパスワード認証プロバイダ１７のチケット解読関数（decodeTicket（認証プライマリチケット））を呼び出す（Ｓ１０５）。なお、パスワード認証プロバイダ１７のチケット解読関数の引数には、認証マージチケットから取り出した認証プライマリチケットが指定される。

【０１２０】

ステップＳ１０５に続いてステップＳ１０６に進み、パスワード認証プロバイダ１７は、引数に指定された認証プライマリチケットの正当性を有効期限及びＭＩＣ等により確認するとともに認証プライマリチケットの内容を解釈し、プライマリチケットの内容をクライアント３０が解釈可能な形式、例えばテキスト形式にした認証情報データ（以下、「プライマリ認証情報データ」という。）を生成する。

【０１２１】

ステップＳ１０６に続いてステップＳ１０７に進み、パスワード認証プロバイダ１７は、生成したプライマリ認証情報データをパスワード・指紋マージプロバイダ１６に出力する。ここで、プライマリ認証情報データを受け取ったパスワー

ド・指紋マージプロバイダ１６は、認証マスタマージチケットが追加認証されたものであるのかを判断する。追加認証されていなければ、認証マスタマージチケットにはこれ以上認証情報は含まれていないため、プライマリ認証情報データがクライアント３０に送信される（Ｓ１０８）。

【０１２２】

一方、既に認証マージチケットについて追加認証を受けている場合は、パスワード・指紋マージプロバイダ１６は、認証マージチケットにマージされている追加チケットを発行した指紋認証プロバイダ１８からも認証情報データを取得するため、指紋認証プロバイダ１８のチケット解読関数（decodeTicket（認証追加チケット））を呼び出す（Ｓ１０９）。

【０１２３】

ステップＳ１０９に続いてステップＳ１１０に進み、指紋認証プロバイダ１８は、引数に指定された認証追加チケットの正当性を有効期限及びＭＩＣ等により確認するとともに認証追加チケットの内容を解釈し、認証情報データ（以下、「追加認証情報データ」という。）を生成する。

【０１２４】

ステップＳ１１０に続いてステップＳ１１１に進み、指紋認証プロバイダ１８は、生成した追加認証情報データをパスワード・指紋マージプロバイダ１６に出力する。ステップＳ１１１に続いてステップＳ１１２に進み、パスワード・指紋マージプロバイダ１６は、パスワード認証プロバイダ１７から取得した追加認証情報データと、指紋認証プロバイダ１８から取得した追加認証情報データとをマージする（以下、マージされた認証情報データを「マージ認証情報データ」という。）。

【０１２５】

図１５は、マージ認証情報データの構成例を示す図である。例えば、マージ認証情報データは、図１５に示されるように、認証サービス名、有効期限、有効範囲、認証プロバイダ、ユーザ識別子、所属グループ、及び主要属性等から構成される。

【０１２６】

認証サービス名は、認証サービスモジュール１１に付けられた名前である。有効期限は、マージチケットに記録されている有効期限である。有効範囲は、プライマリチケット及び追加チケットに記録されている有効範囲をマージしたものである。即ち、「サーバＡ」と「サーバＢ」とがカンマで区切られているが、これは、プライマリチケットはサーバＡで有効であり、追加チケットはサーバＢで有効であることを示している。

【０１２７】

認証プロバイダは、チケットを発行した認証プロバイダの名前の羅列である。「パスワード認証プロバイダ」と「指紋認証プロバイダ」がカンマで区切られているが、これは、パスワード認証プロバイダ１７と指紋認証プロバイダ１８に認証を受けていることを示している。ユーザ識別子は、チケットの発行を受けたユーザを一意に識別するための情報である。所属グループ及び主要属性は、プライマリチケット及び追加チケットの「主なユーザ属性リスト」から抽出した情報をマージしたものである。

【０１２８】

ステップＳ１１２に続いてステップＳ１１３に進み、マージ認証情報データがクライアント３０に送信される（Ｓ１１４）。

【０１２９】

以降、クライアント３０は、取得したマージ認証情報データを確認することにより、クライアントアプリケーション２３のユーザに対して提供可能なサービスを判断することができる。

【０１３０】

更に、図１６は、チケットの第二の利用方法を説明するためのシーケンス図である。図１４においては、クライアント３０がチケットの解読結果を認証情報データとして受け取る例について説明したが、図１６においては、チケットの正当性の確認と、チケットが誰に認証されたのか、あるいはどの程度まで（プライマリ認証まで、又は追加認証まで）認証されているのかを問い合わせる例について説明する。なお、図１６におけるクライアント３０の位置づけは、図１４におけるそれと同じである。

【０１３１】

ステップＳ１２１においてクライアント３０は、プロバイダ呼び分け手段１３の提供するチケット確認関数（ValidateTicket（認証マージチケット））を呼び出すことにより、認証マージチケットの正当性の確認等を認証サーバ１０に要求する。なお、チケット確認関数の引数には、クライアントアプリケーション２３から提示（送信）された認証マージチケットを指定する。

【０１３２】

ステップＳ１２１に続いてステップＳ１２２に進み、チケット確認関数が呼び出されたプロバイダ呼び分け手段１３は、認証マージチケットを発行した認証プロバイダを判別する。

【０１３３】

ステップＳ１２２に続いてステップＳ１２３に進み、プロバイダ呼び分け手段１３は、認証マージチケットの発行元であるパスワード・指紋マージプロバイダ１６を呼び出す。ステップＳ１２３に続いてステップＳ１２４に進み、パスワード・指紋マージプロバイダ１６は、認証マージチケットの正当性を有効期限及びＭＩＣ等により確認し、認証マージチケットにマージされているプライマリチケットを発行したパスワード認証プロバイダ１７のチケット確認関数（ValidateTicket（認証プライマリチケット））を呼び出す（Ｓ１２５）。なお、パスワード認証プロバイダ１７のチケット確認関数の引数には、マージチケットから取り出した認証プライマリチケットが指定される。

【０１３４】

ステップＳ１２５に続いてステップＳ１２６に進み、パスワード認証プロバイダ１７は、引数に指定された認証プライマリチケットの正当性を有効期限及びＭＩＣ等により確認し、確認結果をパスワード・指紋マージプロバイダ１６に出力する（Ｓ１２７）。ここで確認結果とは、例えば、ＴＲＵＥの場合は正当であり、ＦＡＬＳＥの場合は不正であるといったＢＯＯＬ値などでも良い。

【０１３５】

続いて、パスワード・指紋マージプロバイダ１６は、認証マスタマージチケットが追加認証されたものであるのかを判断する。追加認証されていなければ、確

認結果がクライアント３０に送信される（Ｓ１２８）。ここでの確認結果とは、例えば、認証を行った認証プロバイダのプロバイダ名の羅列でもよいし、プライマリプロバイダまでは認証されているといったように、レベルを示すものでもよい。

【０１３６】

一方、既に認証チケットについて追加認証を受けている場合は、パスワード・指紋マージプロバイダ１６は、認証マージチケットにマージされている追加チケットを発行した指紋認証プロバイダ１８に対してもチケットの確認を依頼するため、指紋認証プロバイダ１８のチケット確認関数（ValidateTicket（認証追加チケット））を呼び出す（Ｓ１２９）。

【０１３７】

ステップＳ１２９に続いてステップＳ１３０に進み、指紋認証プロバイダ１８は、引数に指定された認証追加チケットの正当性を有効期限及びＭＩＣ等により確認し、確認結果（例えばＢＯＯＬ値）をパスワード・指紋マージプロバイダ１６に出力する（Ｓ１３１）。ステップＳ１３１に続いてステップＳ１３２に進み、パスワード・指紋マージプロバイダ１６は、パスワード認証プロバイダ１７と指紋認証プロバイダ１８とから取得した確認結果をマージしたものをクライアント３０に対する確認結果としてプロバイダ呼び分け手段１３に出力する。例えば、ここでの確認結果とは、認証を行った認証プロバイダのプロバイダ名の羅列でもよいし、追加プロバイダまでは認証されているといったように、レベルを示すものでもよい。

【０１３８】

ステップＳ１３２に続いてステップＳ１３３に進み、プロバイダ呼び分け手段１３は、確認結果をクライアント３０に送信する。

【０１３９】

確認結果を受信したクライアント３０、確認結果に基づいて、クライアントアプリケーション２３のユーザに対して提供可能なサービスを判断することができる。

【０１４０】

上述したように、本実施の形態における認証サーバ１０によれば、マージプロバイダが、認証プロバイダマージテーブル１９４によって、プライマリＩＤから追加ＩＤを導出し、かかる追加ＩＤに基づいて追加認証をおこなうため、プライマリ認証を受けたユーザと追加認証を受けようとしているユーザの同一性を保証し、当該ユーザが本人であることの保証をより高めることができる認証サービスを提供することができる。

【０１４１】

また、認証した結果は、チケットとして発行され、当該チケットは、有効範囲、有効期限、改竄チェック用のコードを有しているため、より高度なセキュリティを確保することができる。即ち、有効範囲で、利用可能なシステム等が制限され、有効期限によって、利用可能な期間が制限され、改竄チェック用のコードによって、チケットの正当性が担保されるからである。

【０１４２】

また、プライマリプロバイダや追加プロバイダが発行したチケットは、マージプロバイダによってマージチケットにマージされて発行されるため、チケットを発行された側は、各チケットの関連付けについて関与する必要はなく、チケットの取り扱いを容易にすることができる。

【０１４３】

なお、本実施の形態においては、認証サービスモジュール１１が、ネットワークを介して接続されている端末２０に配置されているクライアントアプリケーション２３に対して認証機能を提供する例について説明したが、本発明は、かかるクライアント・サーバ型のシステムに限定されるものではない。

【０１４４】

図１７は、内部アプリケーションに認証機能を提供する場合の認証サーバの機能構成例を示す図である。図１７中、図１と同一部分には同一符号を付し、その説明は省略する。図１７においては、アプリケーション４１、４２、４３、及び４４が、ＳＯＡＰ経由ではなく、プロバイダ呼び分け手段１３の関数を直接呼び出すように構成されている。このように、認証サーバ１０の内部に構築したアプリケーションからも、認証サービスモジュール１１を利用することができる。

【０１４５】

以上、本発明の好ましい実施例について詳述したが、本発明は係る特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

【０１４６】

【発明の効果】

上述の如く、本発明によれば、ユーザの同一性を保証しつつ複数の認証機能によってユーザを認証することができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態における認証システムの構成例を示す図である。

【図２】

マージ情報管理ＤＢを構成する認証プロバイダ管理テーブルの構成例を示す図である。

【図３】

マージ情報管理ＤＢを構成するマージプロバイダ管理テーブルの構成例を示す図である。

【図４】

マージ情報管理ＤＢを構成する追加プロバイダ管理テーブルの構成例を示す図である。

【図５】

マージ情報管理ＤＢを構成する認証プロバイダマージテーブルの構成例を示す図である。

【図６】

外部認証サーバにおけるユーザ管理テーブルの構成例を示す図である。

【図７】

指紋ＤＢを構成する指紋特徴データ管理テーブルの構成例を示す図である。

【図８】

本発明の実施の形態における認証サーバのハードウェア構成例を示す図である

。

【図９】

プライマリ認証の際の認証サーバの処理を説明するためのシーケンス図である。

【図１０】

通常のチケットのデータ構造の例を示す図である。

【図１１】

マージチケットのデータ構造の例を示す図である。

【図１２】

追加認証の際の認証サーバの処理を説明するためのシーケンス図である。

【図１３】

追加認証の際の認証サーバの処理を説明するためのシーケンス図である。

【図１４】

チケットの第一の利用方法を説明するためのシーケンス図である。

【図１５】

マージ認証情報データの構成例を示す図である。

【図１６】

チケットの第二の利用方法を説明するためのシーケンス図である。

【図１７】

内部アプリケーションに認証機能を提供する場合の認証サーバの機能構成例を示す図である。

【符号の説明】

１　　認証システム

１０　　認証サーバ

１１　　認証サービスモジュール

１２　　ＳＯＡＰスタブ

１３　　プロバイダ呼び分け手段

１４　　認証プロバイダＡ

１５　　認証プロバイダＢ

１６　　パスワード・指紋マージプロバイダ

１７　　パスワード認証プロバイダ

１８　　指紋認証プロバイダ

１９　　マージ情報管理ＤＢ

２０　　端末

２２　　ＳＯＡＰプロキシ

２３　　クライアントアプリケーション

２４　　指紋読み取り装置ドライバ

２５　　指紋読み取り装置

４０　　外部認証サーバ

１００　ドライブ装置

１０１　記憶媒体

１０２　補助記憶装置

１０３　メモリ装置

１０４　演算処理装置

１０５　インタフェース装置

１８１　指紋認証ライブラリ

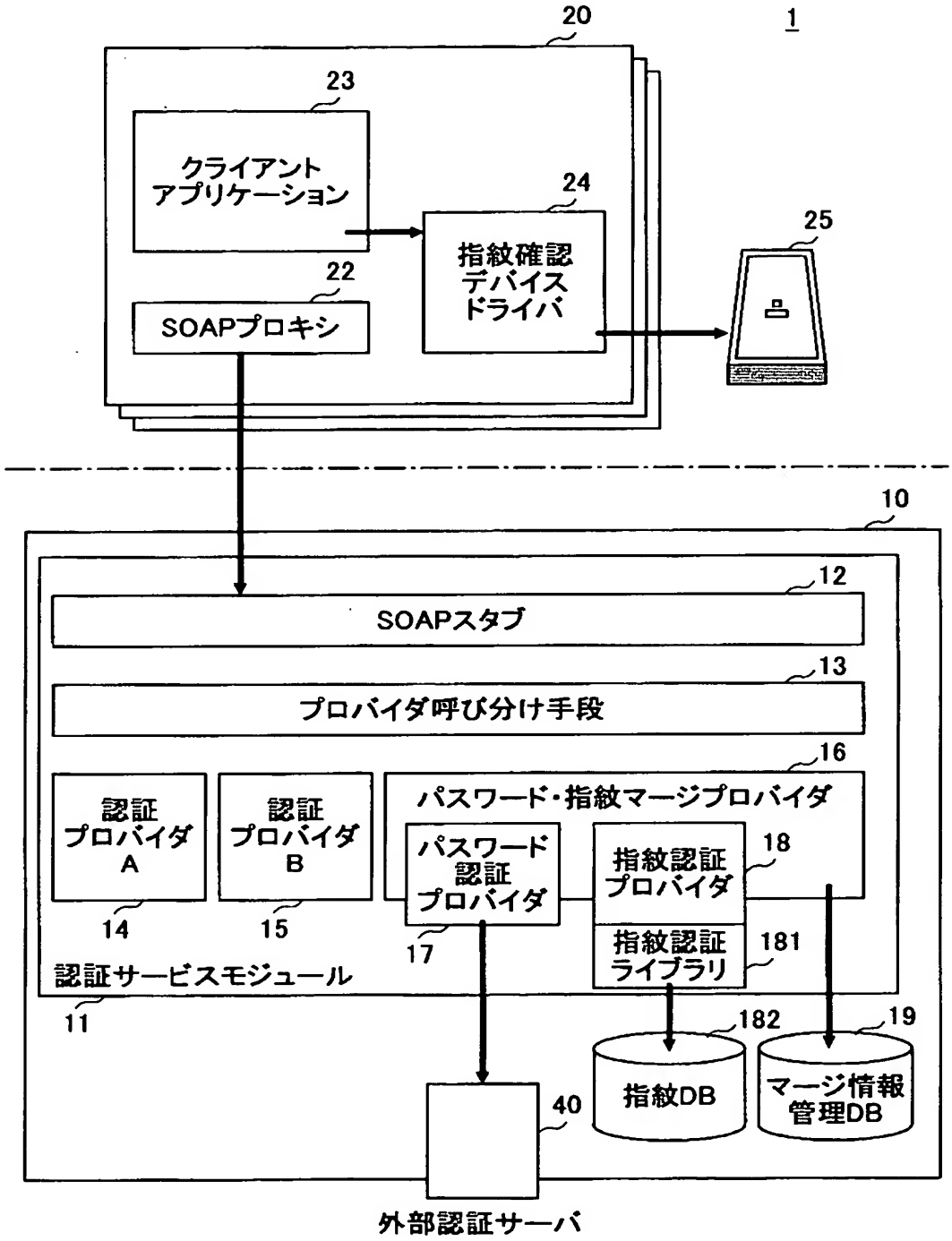
１８２　指紋ＤＢ

Ｂ　　バス

【書類名】　図面

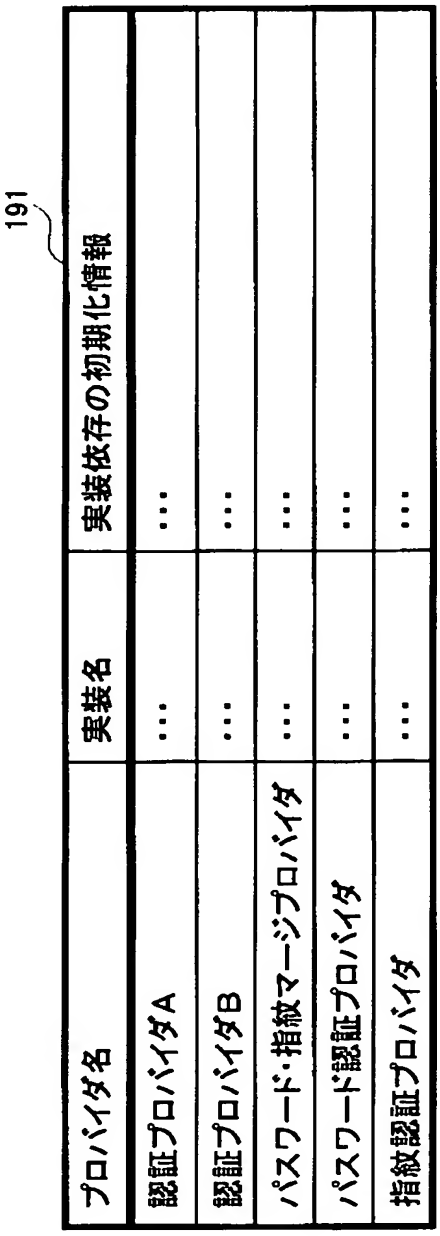
【図１】

本発明の実施の形態における認証システムの構成例を示す図



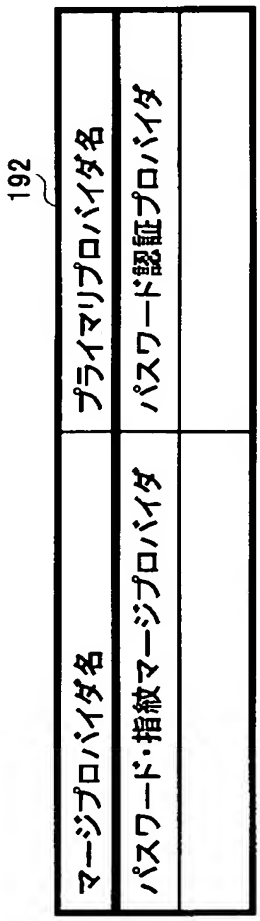
【図２】

マージ情報管理DBを構成する
認証プロバイダ管理テーブルの構成例を示す図



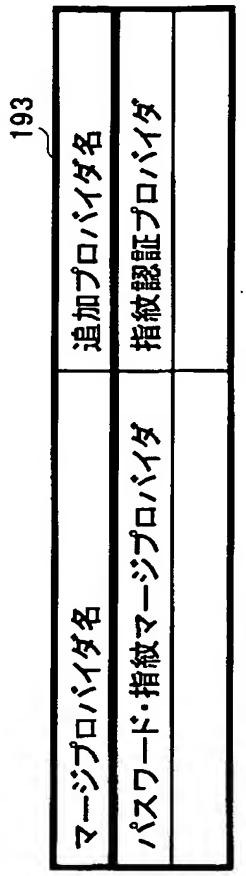
【図３】

マージ情報管理DBを構成する
マージプロバイダ管理テーブルの構成例を示す図



【図４】

マージ情報管理DBを構成する
追加プロバイダ管理テーブルの構成例を示す図



【図５】

マージ情報管理DBを構成する
認証プロバイダマージテーブルの構成例を示す図

194

マージプロバイダ名	プライマリID	追加プロバイダ名	追加ID
パスワード・指紋マージプロバイダ	0001	指紋認証プロバイダ	5551
パスワード・指紋マージプロバイダ	0002	指紋認証プロバイダ	5552
パスワード・指紋マージプロバイダ	0003	指紋認証プロバイダ	5553
：	：	：	：

【図６】

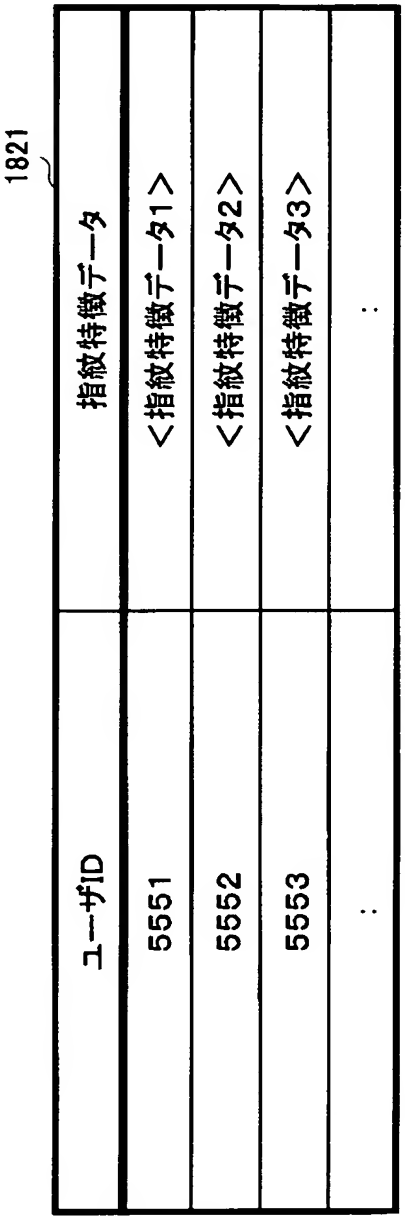
外部認証サーバにおけるユーザ管理テーブルの構成例を示す図

41

ユーザID	パスワード	氏名	…
0001	*****	XXXXX	..
0002	*****	YYYYYY	..
0003	*****	ZZZZZZZ	..
..	..	..	..

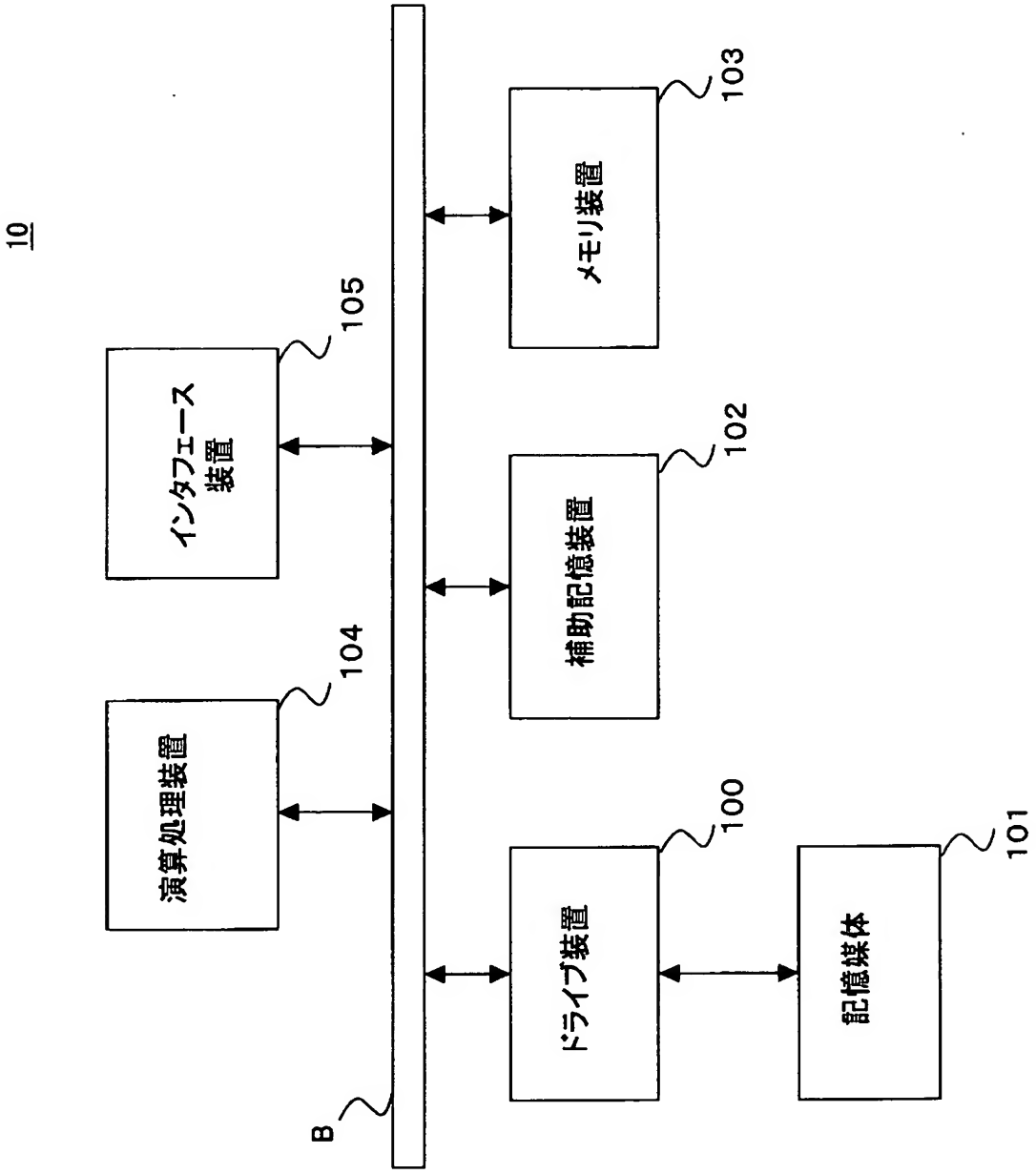
【図７】

指紋DBを構成する指紋特徴データ管理テーブルの構成例を示す図



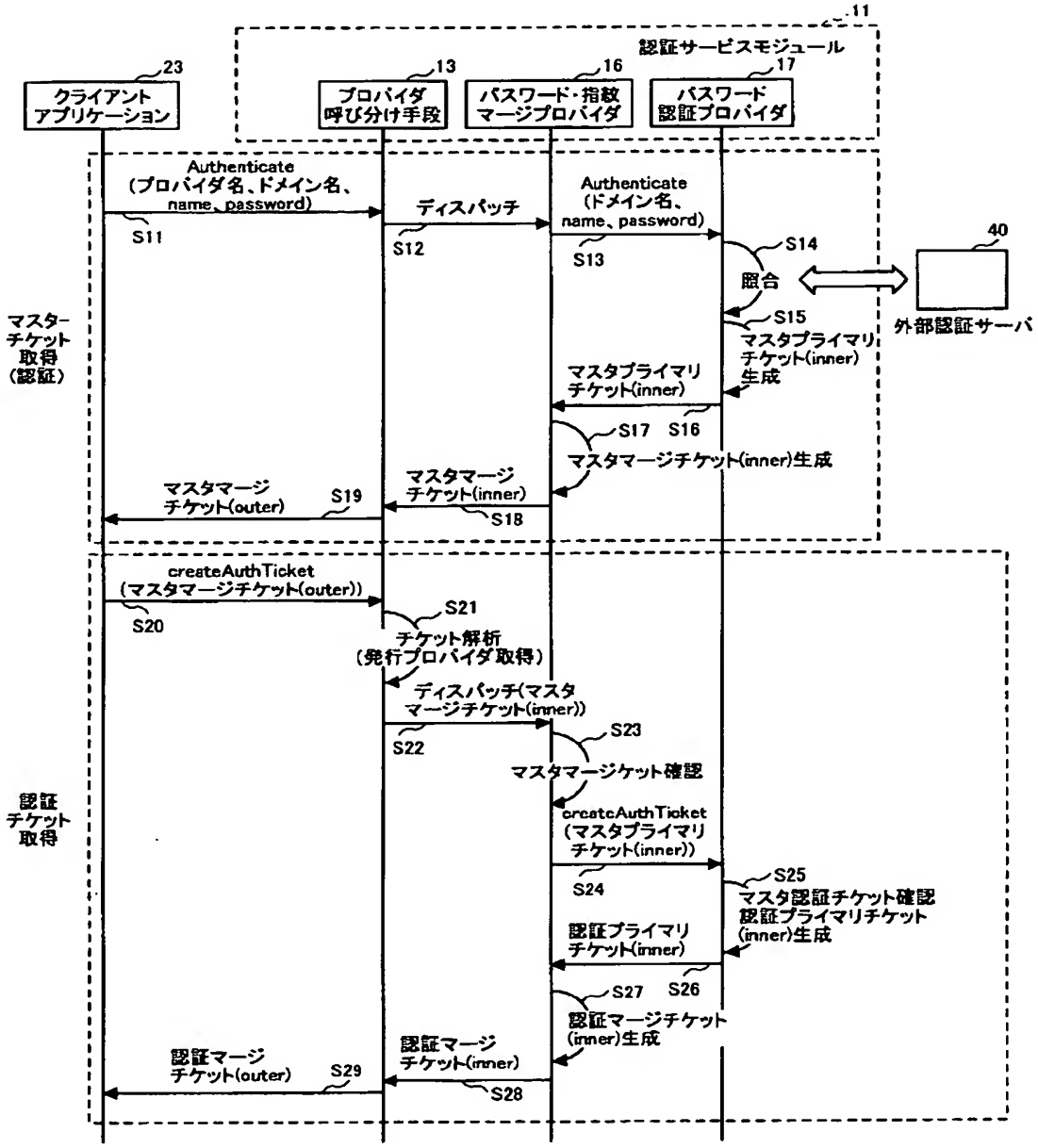
【図８】

本発明の実施の形態における
認証サーバのハードウェア構成例を示す図



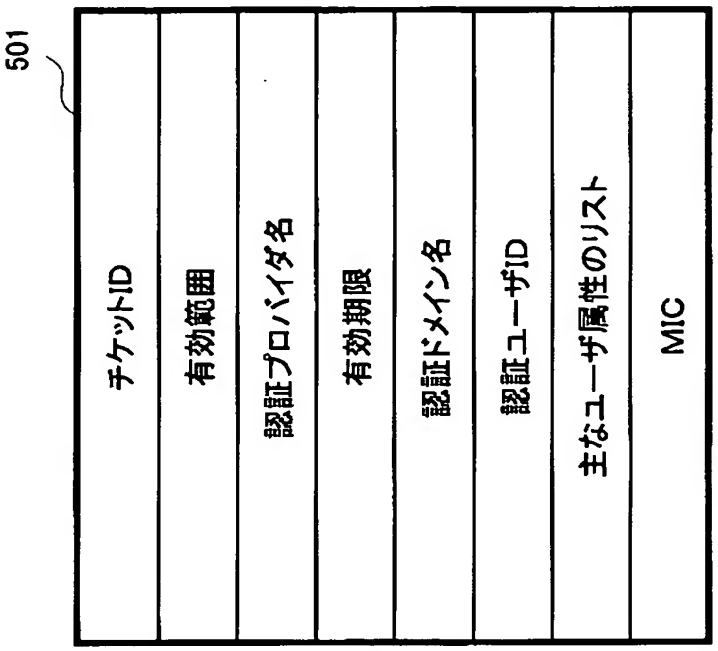
【図９】

プライマリ認証の際の認証サーバの処理を
説明するためのシーケンス図



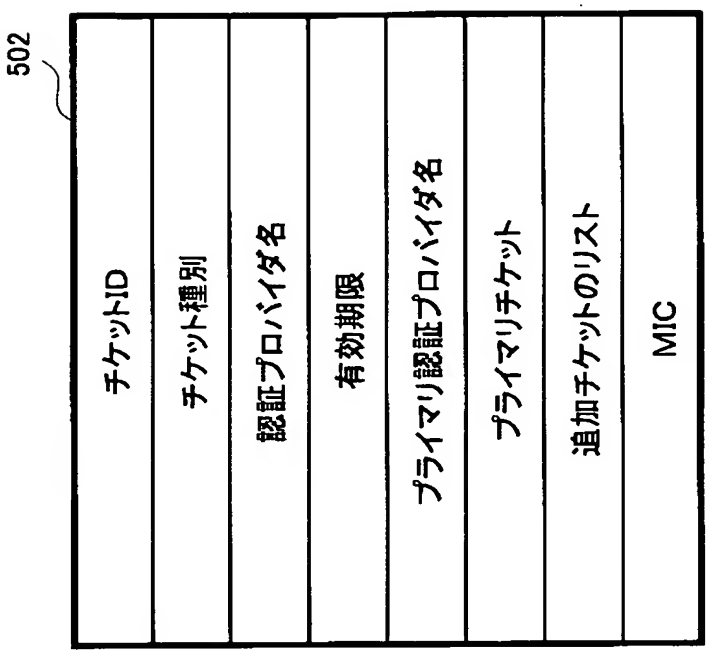
【図１０】

通常のチケットのデータ構造の例を示す図



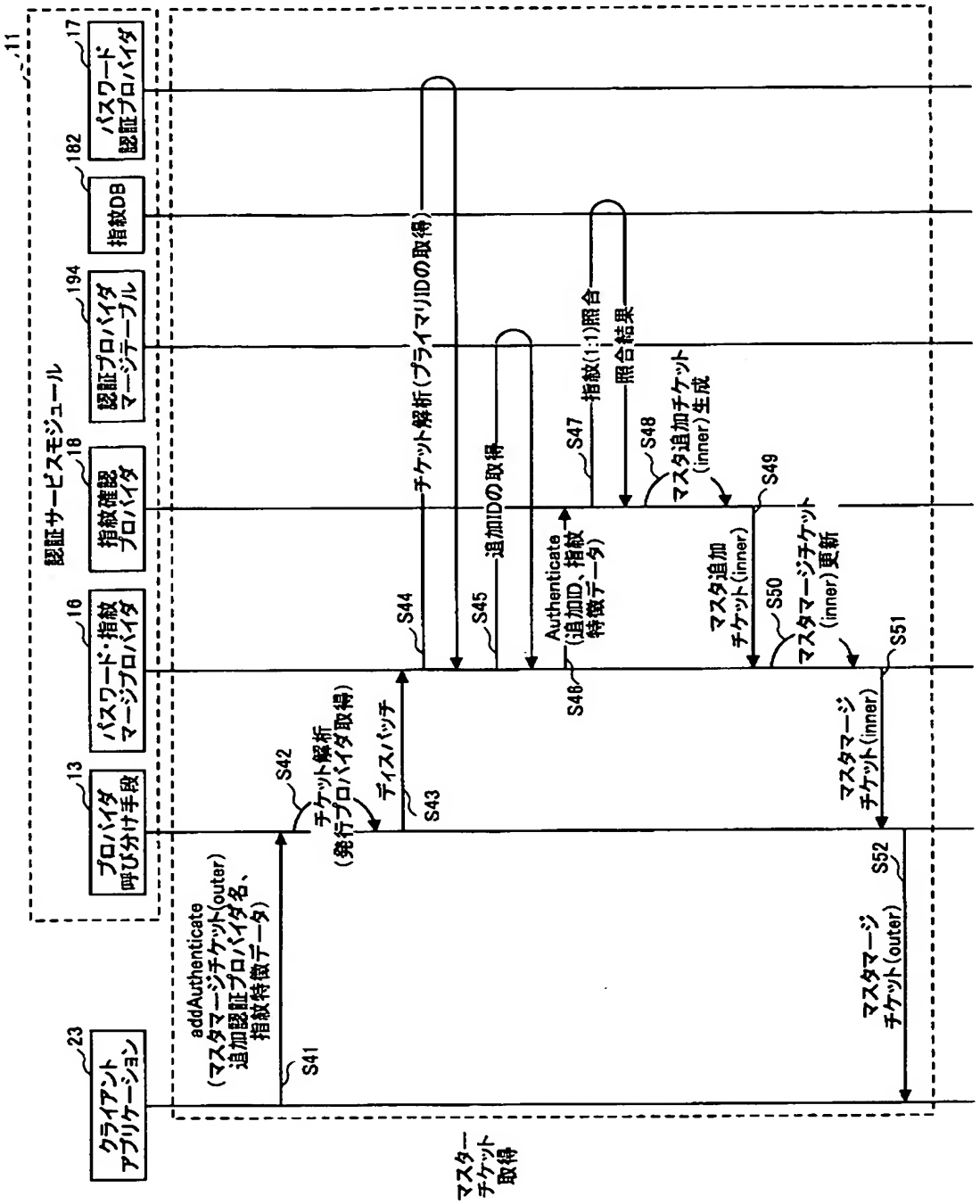
【図１１】

マージチケットのデータ構造の例を示す図



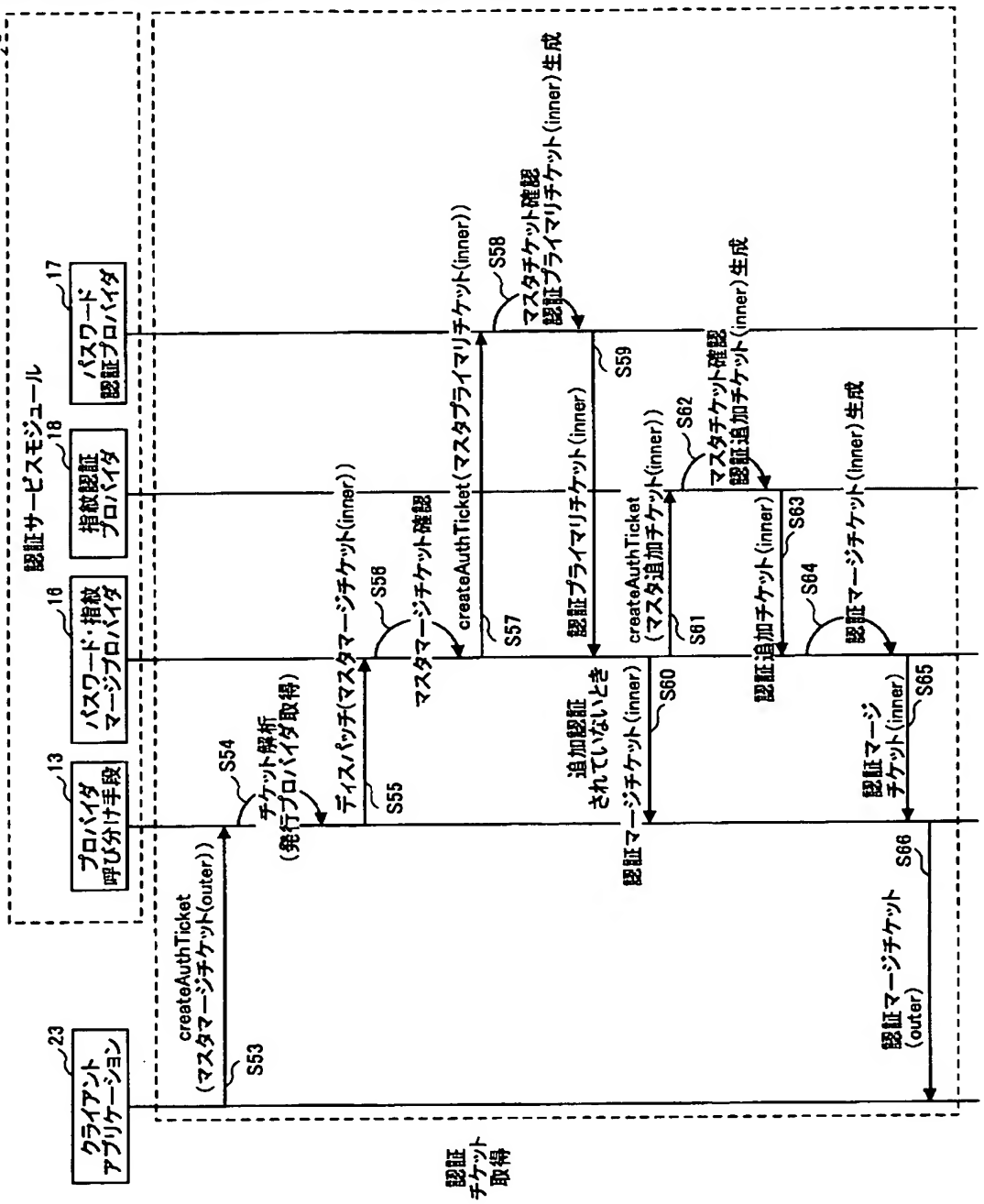
【図１２】

追加認証の際の認証サーバの処理を説明するためのシーケンス図



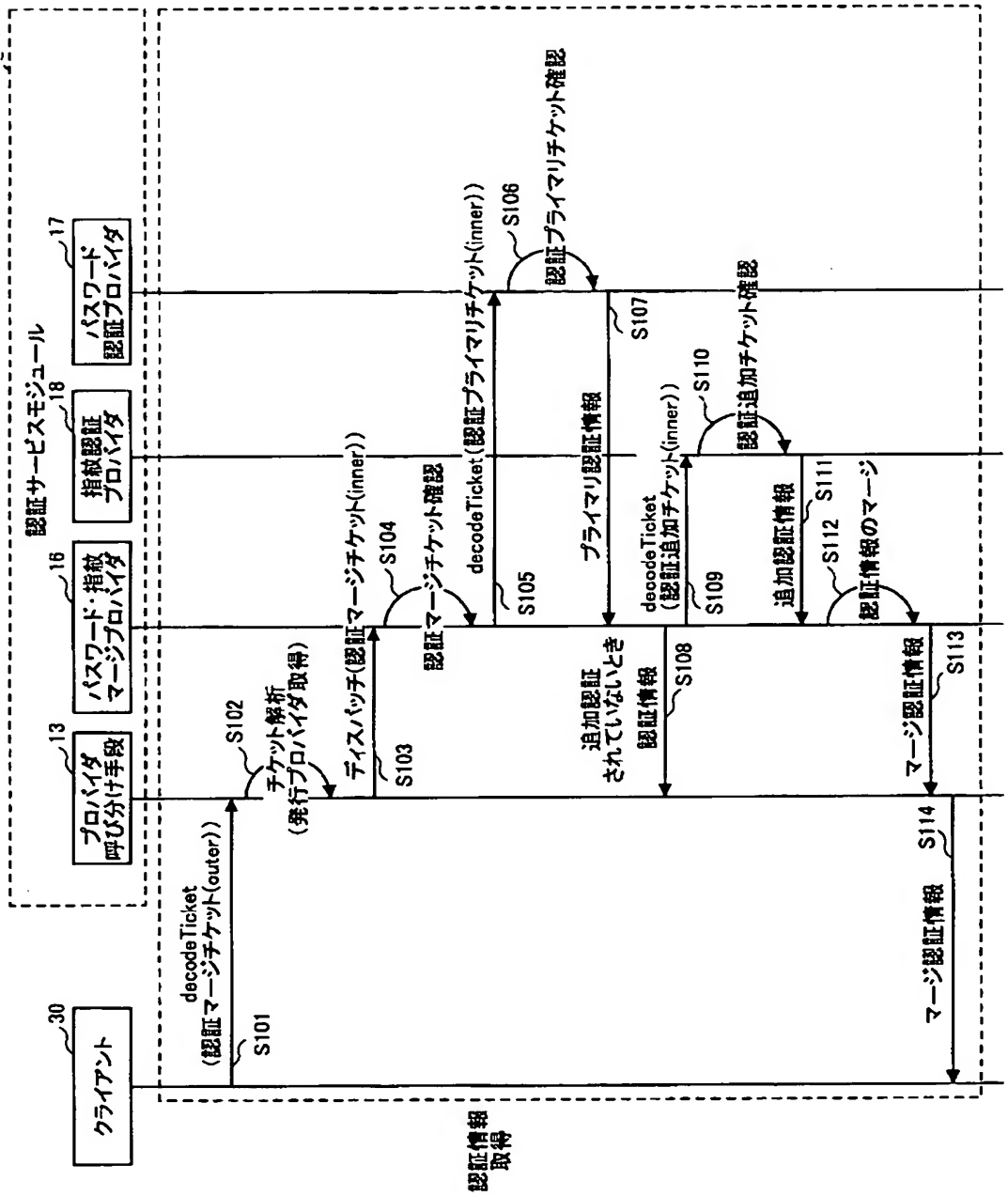
【図１３】

追加認証の際の認証サーバの処理を説明するためのシーケンス図



【図１４】

チケットの第一の利用方法を説明するためのシーケンス図



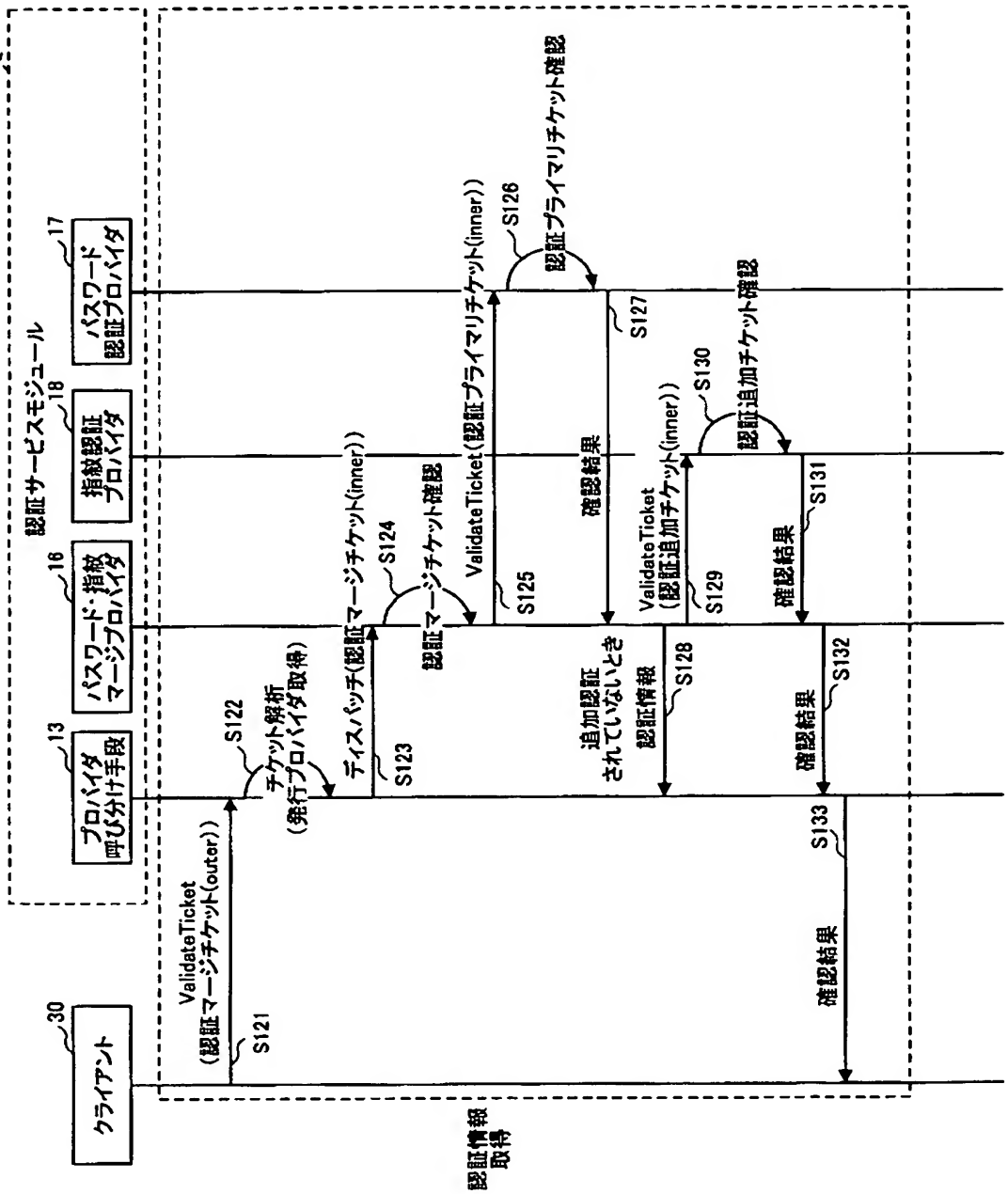
【図１５】

マージ認証情報データの構成例を示す図

認証サービス名	"UauthService01.RRR"
有効期限	2003/02/07:18:31:12
有効範囲	"サーバA"、"サーバB"
認証プロバイダ	"パスワード認証プロバイダ"、 "指紋認証プロバイダ"
ユーザ識別子	S-001-719964-772588612
所属グループ	Users, SscMembers, sgAdmin, fp_exclusive
主要属性	post=manager, class=AC, mail=xxx.rrr.co.jp

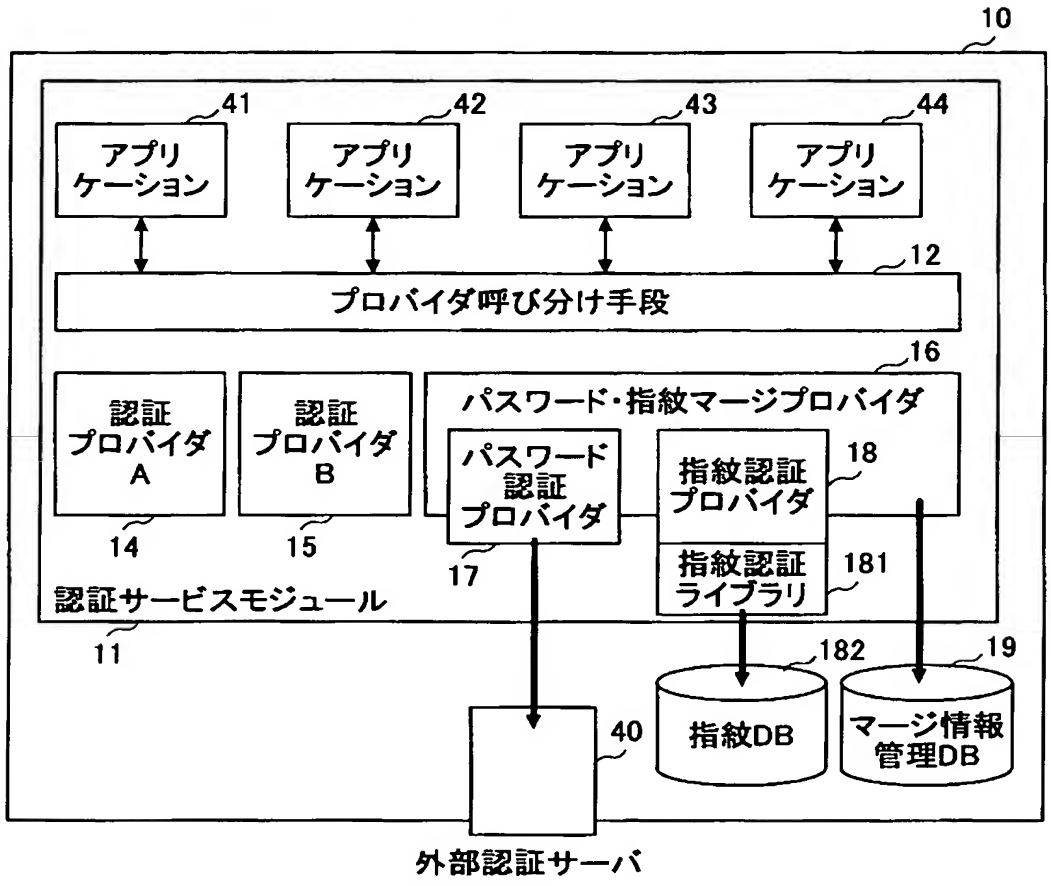
【図１６】

チケットの第二の利用方法を説明するためのシーケンス図



【図１７】

内部アプリケーションに認証機能を提供する場合の
認証サーバの機能構成例を示す図



【書類名】　　要約書

【要約】

【課題】　ユーザの同一性を保証しつつ複数の認証機能によってユーザを認証することができるユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体の提供を目的とする。

【解決手段】　ユーザの認証を行う複数の認証手段を連携させる連携手段を有するユーザ認証装置であって、前記連携手段は、クライアントからのユーザの第一の認証要求に応じて、第一の認証手段に認証要求において指定された第一のユーザ識別情報に基づいてユーザを認証させる第一の呼び出し手段と、クライアントからの、第一の認証手段に認証されているユーザの第二の認証要求に応じて、第一のユーザ識別情報に予め対応づけられた、第二の認証手段におけるユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手段と、第二の認証手段にユーザ識別情報検索手段が検索した第二のユーザ識別情報に基づいてユーザを認証させる第二の呼び出し手段とを有することにより上記課題を解決する。

【選択図】　　図１

特願２００３－０７８９９３

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー